METODOLOGÍA PARA LA OPTIMIZACIÓN EN LA GESTIÓN DE VULNERABILIDADES EN BANCO DE OCCIDENTE

JUAN GUILLERMO CASAS PINTO
DAVID FERNANDO RAMÍREZ LEÓN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

METODOLOGÍA PARA LA OPTIMIZACIÓN EN LA GESTIÓN DE VULNERABILIDADES EN BANCO DE OCCIDENTE

JUAN GUILLERMO CASAS PINTO
DAVID FERNANDO RAMÍREZ LEÓN

Proyecto de Grado para optar al título de Especialista en Seguridad Informática

Tutor
ÁLVARO ESCOBAR ESCOBAR
Director Especialización en Seguridad Informática
Director Especialización en Telecomunicaciones

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C. Febrero de 2018

A nuestras familias
quienes a lo largo de nuestro
proyecto nos han apoyado y
motivado en nuestra formación
académica,

AGRADECIMIENTOS

Este proyecto es el resultado del esfuerzo y la dedicación conjunta de quienes formamos este equipo de trabajo por esto agradecemos:

A Dios puesto que de su mano nada es imposible.

De manera muy especial a nuestro Tutor del Proyecto de grado Álvaro Escobar Escobar quien con su orientación y apoyo nos supo guiar en nuestro proyecto.

A los docentes que han apoyado esta iniciativa con sus valiosos aportes desde su conocimiento y experiencia.

A la Universidad la cual abrió sus puertas preparándonos para un futuro competitivo.

CONTENIDO

LISTA DE CUADROS

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: dispositivo o elemento que almacena, procesa o transmite información en la infraestructura tecnológica de una empresa u organización[1].

ANÁLISIS DE VULNERABILIDAD: proceso sistemático para estimar la debilidad de un activo o grupo de activos de información que puede ser aprovechado por un atacante[2].

ATAQUE CIBERNETICO: Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio[3].

HARDENING: proceso de asegurar un sistema mediante la reducción de vulnerabilidades[4].

INFRAESTRUCTURA: conjunto de dispositivos, servicios e instalaciones requeridos para el desarrollo de una actividad[5].

MALWARE: código malicioso diseñado para infiltrarse en activos de información sin consentimiento del propietario[6].

VULNERABILIDAD: error o debilidad, que de llegar a explotarse, puede ocasionar una exposición a riesgos del sistema, intencionalmente o no[7].

---

[1] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE COLOMBIA. Guía para la gestión y clasificación de activos de información – MinTic. . (Citado el 21 de Noviembre de 2017). Disponible en Internet: < (https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf>

[2] WELIVESECURITY. Análisis de vulnerabilidad. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < www.welivesecurity.com.

[3] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE COLOMBIA. Modelo nacional de gestión de riesgos de seguridad digital. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <www.mintic.gov.co/portal/604/articles-61854_documento.docx.

[4] Ibíd. p. 17

[5]DEFINICIÓN ABC. Definición Infraestructura. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.definicionabc.com

[6] INFOSPY WARE. Definición Malware. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.infospyware.com

[7] SECURITY STADARDS COUNCIL. Definición de vulnerabilidad. Citado el 21 de Noviembre de 2017). Disponible en Internet: < (https://es.pcisecuritystandards.org)

NIVEL DE EXPOSICIÓN: medida de la frecuencia con que se da la exposición al riesgo[8].

TARJETAHABIENTE: Persona poseedora de tarjeta de crédito o débito[9].

CVSS - Common Vulnerability Scoring System: El sistema de puntuación de vulnerabilidades común, es un modelo cuantitativo el cual permite a los usuarios de TI generar una medición de las debilidades presentes en los sistemas de información[10].

[8] JIMÉNEZ, Milenys. Seguridad e Higiene Industrial SHI. Universidad Nacional Abierta. Centro LOCAL Cojedes, Citado el 21 de Noviembre de 2017). Disponible en Internet: < shi-unacojedes.wikispaces.com/Nivel+de+Exposición.

[9] REAL ACADEMIA ESPAÑOLA-RAE. (2014). Tarjetahabiente. (33 ed.). Madrid: ASALE.

[10] WELIVESECURITY. Vulnerabilidades-que-es-cvss-como-utilizarlo. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

INTRODUCCIÓN

El presente documento plantea una metodología que permite priorizar el orden de remediación de las vulnerabilidades identificadas en los sistemas de los activos de información al interior del Banco de Occidente, las cuales fueron previamente halladas por la herramienta de software (QRADAR[11]), sin embargo la información arrojada por dicho sistema es insuficiente para facilitar la gestión de vulnerabilidades encontradas y se hace necesario realizar esfuerzos adicionales con el fin de remediar los hallazgos encontrados, para ello se dará a conocer la importancia de realizar una priorización de dichas vulnerabilidades con el fin de minimizar de forma objetiva el tiempo de exposición de las vulnerabilidades más críticas para la entidad.

La gestión de vulnerabilidades es el tratamiento que se realiza a las plataformas tecnológicas, con el fin de mitigar los riesgos de materialización de ataques a los sistemas; estas se centran en llevar a cabo procesos de identificación, clasificación y mitigación de amenazas.

Dentro de las compañías que gestionan vulnerabilidades de seguridad informática, quien tiene una propuesta de valor respecto a priorización de amenazas es RAN SECURITY[12], esta compañía se especializa en realizar escaneos de vulnerabilidades en diferentes entornos. De acuerdo a la investigación realizada por la compañía RAN SECURTIY el número de hallazgos encontrados por gestión va de decenas a cientos. Sin embargo, se desconoce si RAN SECURITY tiene establecido un plan de acción por segmento económico, la dinámica que utiliza para dar un valor agregado al que brindan los sistemas de gestión de vulnerabilidades tradicionales.

Mediante la circular 029 emitida por la Superintendencia Financiera de Colombia, se establecen los requerimientos mínimos de seguridad que están obligados a cumplir las entidades del sector financiero colombiano, dicha circular establece que realicen como mínimo dos escaneos de vulnerabilidades anuales. Banco de Occidente en cumplimiento de lo establecido en la circular, frente a la evaluación de vulnerabilidades en sus sistemas de información ejecuta semestralmente esta

[11] QRadar (tm) es una plataforma de gestión de seguridad de red que por medio de escaneos (firmas) identifica las vulnerabilidades conocidas en la infraestructura tecnológica de una organización.

[12] RAN SECURITY. Compañía creada en 1991 especializada en soluciones de seguridad y gestión de la información. Actualmente opera en Argentina, Chile, Perú, Paraguay, Colombia y México.

actividad, el resultado de este ejercicio identifica las posibles amenazas potenciales que tienen las plataformas tecnológicas, estas vulnerabilidades deben ser gestionadas en el menor tiempo posible dando prioridad a aquellas que se encuentren en activos que están sujetos a una regulación (SOX[13]). Las amenazas identificadas en el proceso de gestión de vulnerabilidades están directamente relacionadas con los riesgos a los cuales que están expuestas las organizaciones que pueden llegar a comprometer la continuidad del negocio.

Debido a que los volúmenes de hallazgos encontrados son altos, la objetividad de priorización a menudo se limita; los escaneos tradicionales basan la importancia de las amenazas en rangos predefinidos, como la *CVE[14], WHOIS[15] CERT*[16], SANS[17], entre otras, sin tener en cuenta el valor de los activos de información que representan para la organización. La metodología actual que el banco utiliza puede solucionar aspectos no amenazantes o también estar dando una prioridad baja e incluso ignorar aspectos críticos para la compañía, obteniendo como resultado una gestión de vulnerabilidades insuficiente.

Para que sean eficaz la remediación de vulnerabilidades en las plataformas informáticas, además de la herramienta que realiza y clasifica los hallazgos por criticidades ya establecidas, se hace necesario optar por una metodología que permita priorizar las vulnerabilidades de acuerdo al entorno de la Organización.

De esta forma se gestionan los hallazgos verdaderamente importantes, evitando perdidas de dinero, esfuerzos operativos, dando como resultado la reducción del tiempo de exposición de una amenaza critica para la entidad.

---

[13] SOX. Ley Sarbanes Oxley. nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

[14] CVE. Common Vulnerabilities and Exposures: lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.

[15] WHOIS. Sistema de consulta de información pública asociada a recursos de Internet tales como registros de nombres de dominio o direcciones de red.

[16] CERT. Colección de información de seguridad de Internet relacionados con incidentes y vulnerabilidades.

[17] SANS. institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática, dedicados a certificar en el ámbito de seguridad informática.

1. PLANTEAMIENTO DEL PROBLEMA

¿Cómo el Banco de Occidente puede identificar y priorizar la gestión de las vulnerabilidades que generan más riesgo a su infraestructura y así minimizar los niveles de exposición?

El Banco de Occidente una vez efectúa los escaneos de vulnerabilidades (ordenados por la norma 029 emanada por la Superintendencia Financiera de Colombia), que se ejecutan con la herramienta *QRadar*, la cual evidencia un alto número de hallazgos que han sido identificados. Estas vulnerabilidades crecen en forma exponencial a medida que incrementa su infraestructura tecnológica.

El Banco de Occidente gestiona un plan de acción de acuerdo a la criticidad de las vulnerabilidades encontradas en la cual inicia por los hallazgos cuya valoración esta como critica para los activos que tienen cumplimiento SOX y finalizando con las vulnerabilidades clasificadas como bajas. De igual manera realizan bimestralmente un comité de vulnerabilidades con los administradores de las plataformas tecnológicas, donde su objetivo es validar el estado de la gestión a las amenazas encontradas y de esta forma obtener un “status”.

Sin embargo, al tener un número tan alto de hallazgos y contar con un recurso humano limitado, que en algunos casos por la falta de conocimiento del negocio por parte de los administradores hacen que al momento de gestionar las vulnerabilidades no se tenga la certeza que aquellas identificadas como críticas sean las más significativas y relevantes desde el punto de vista de riesgo para la Entidad.

2. JUSTIFICACIÓN

En cumplimiento de la circular 029 emitida por la Superintendencia Financiera de Colombia, el Banco de Occidente[18] debe efectuar escaneos de vulnerabilidades con una determinada periodicidad.

Como medida preventiva, gestionan los hallazgos encontrados con base en la herramienta adquirida para dicho propósito (escáner de vulnerabilidades - **QRADAR**), dicho dispositivo clasifica las vulnerabilidades según la información registrada en la lista ***CVE***, está clasificación tiene en cuenta factores como:

- Exposición de la información en el activo en que reposa,
- Confidencialidad,
- Integridad,
- Disponibilidad,
- Facilidad de explotación,
- Publicación de *exploit*[19],
- Entre otros.

Sin embargo, se evidencia que algunas amenazas que se catalogan mediante este mecanismo, proporciona una prioridad que para la criticidad de sus activos no es la realidad. Vulnerabilidades con criticidad crítica o alta que no tienen mayor impacto para la organización o vulnerabilidades con criticidad media o baja, que en el evento de ser explotadas por un atacante tienen un impacto importante para la misma, razón por la cual deben ser gestionadas con la misma prioridad que los hallazgos críticos.

En el presente documento se plantea una metodología que pretende mejorar la priorización en la gestión de las vulnerabilidades, posterior a la identificación que realiza la herramienta que las detecta. La propuesta de valor es focalizar la gestión, minimizando la perdida de esfuerzo y tiempo dedicado a tratar vulnerabilidades que no representan alto riesgo para la organización, de esta forma se optimiza el recurso humano, se reducen costos y se mejora la postura de seguridad del Banco reduciendo así el nivel de exposición presente en su infraestructura.

---

[18] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 029/14 Bogotá D.C. Superfinanciera. 2014. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <https://www.google.com.co/search?dcr=0&ei=d2VrWvikHIjyzgK-qp_4Bw&q=circular+029+emitida+por+la+Superintendencia+Financiera+de+Colombia%2C+el+Banco+de+Occidente&gs_l=psy-ab.3...4821862.4822963.0.4824880.1.1.0.0.0.0.145.145.0j1.1.0....0...1c.1.64.psy-ab..0.0.0

[19] Exploit. fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Crear una metodología que permita al Banco de Occidente identificar las vulnerabilidades con mayor impacto para la organización, con el fin de optimizar de manera eficaz la gestión de vulnerabilidades y así reducir la probabilidad de materialización de riesgos por un ataque.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer indicadores mediante una formulación matemática que permita mejorar la priorización de la criticidad de las vulnerabilidades.

- Identificar las herramientas que permitan obtener la información necesaria para realizar el análisis planteado.

- Crear un esquema cuantitativo para los diferentes criterios de análisis, valor de criticidad, valor del activo, valoración en la red.

- Identificar vulnerabilidades en la infraestructura de la entidad.

- Consolidar y clasificar los activos de información de acuerdo al esquema cuantitativo.

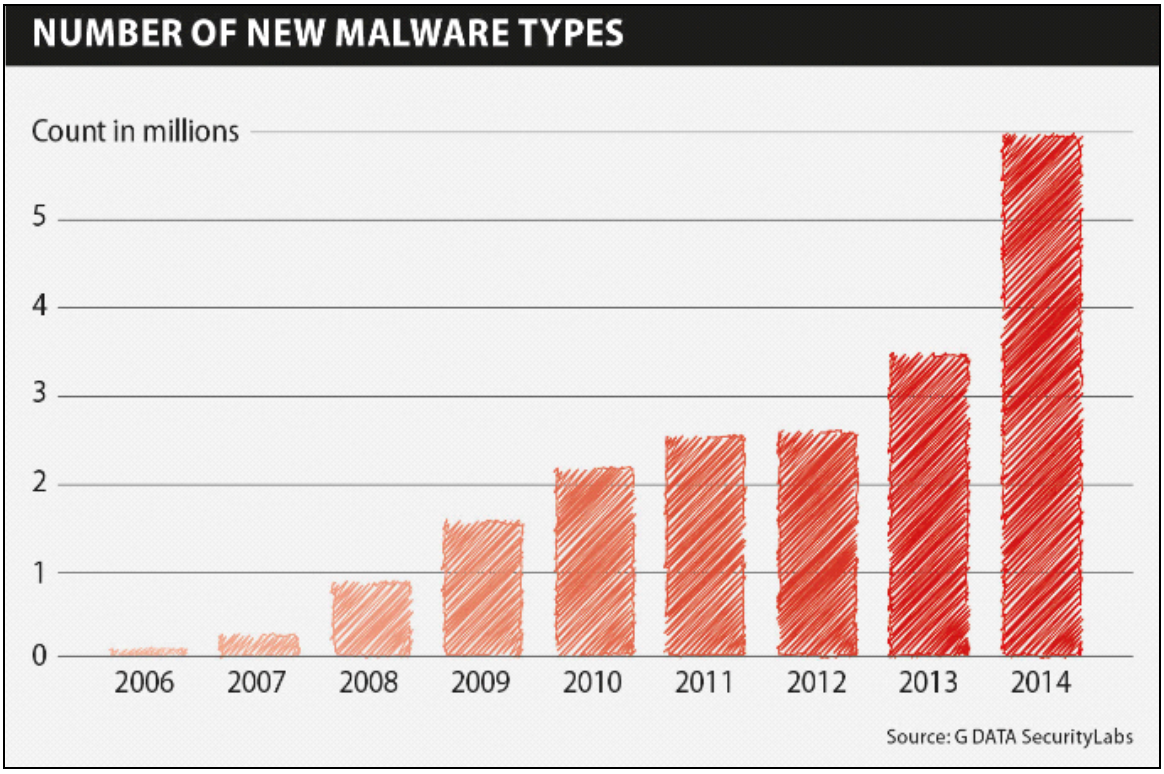
- Evaluar y analizar la metodología propuesta vs la actual.

4. MARCO TÉORICO

El desarrollo de las tecnologías y su masificación aparecen en respuesta de la globalización de los mercados con la intención de ofrecer nuevos productos, servicios o beneficios para sus usuarios, sin embargo, a medida que evolucionan las tecnologías de la información también lo hacen las vulnerabilidades en los mismos. De acuerdo a lo anterior se afirma que las vulnerabilidades crecen en el mismo sentido a la infraestructura, su cantidad se incrementa de manera exponencial, aumentando el interés por parte de los atacantes.

Es importante destacar que los tipos de malware también han evolucionado y aumentado significativamente como se puede observar en la Gráfica 1; lo cual exige a las organizaciones una búsqueda permanente para "protegerse", cerrando las brechas que puedan existir en su infraestructura por las vulnerabilidades presentes y minimizando los eventos mediante los cuales un atacante puede tomar como objetivo una vulnerabilidad y explotarla.

Gráfica 1. Número de nuevos tipos de malware



Fuente. TILVES, Mónica. Cada 3.75 segundos surge un nuevo malware Windows. Silicon. 2015. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <. http://www.silicon.es/cada-375-segundos-surge-un-nuevo-malware-para-windows-82057

Teniendo presente la evolución del malware, algunas organizaciones nacen a partir de la necesidad de crear un repositorio de consulta a nivel mundial donde se brinde información respecto a las vulnerabilidades detectadas en las tecnologías, de manera que permitan clasificarlas de acuerdo a unos criterios, que sirvan como insumo para fabricantes de herramientas de escaneos de vulnerabilidad. En la actualidad existen varias bases de datos que manejan dicha información, con diferentes criterios de evaluación para las vulnerabilidades.

4.1 BASES DE DATOS DE VULNERABILIDADES

Algunas de las bases de datos de vulnerabilidades para el CVSS públicamente conocidas son; *National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB).* Aunque cada una de las anteriores difiere en algunos criterios al momento de evaluar las vulnerabilidades, dicha evaluación es un primer insumo para que las organizaciones tengan un valor inicial de los posibles riesgos a los que se encuentran expuestos.

4.2 ¿QUÉ ES CVSS?

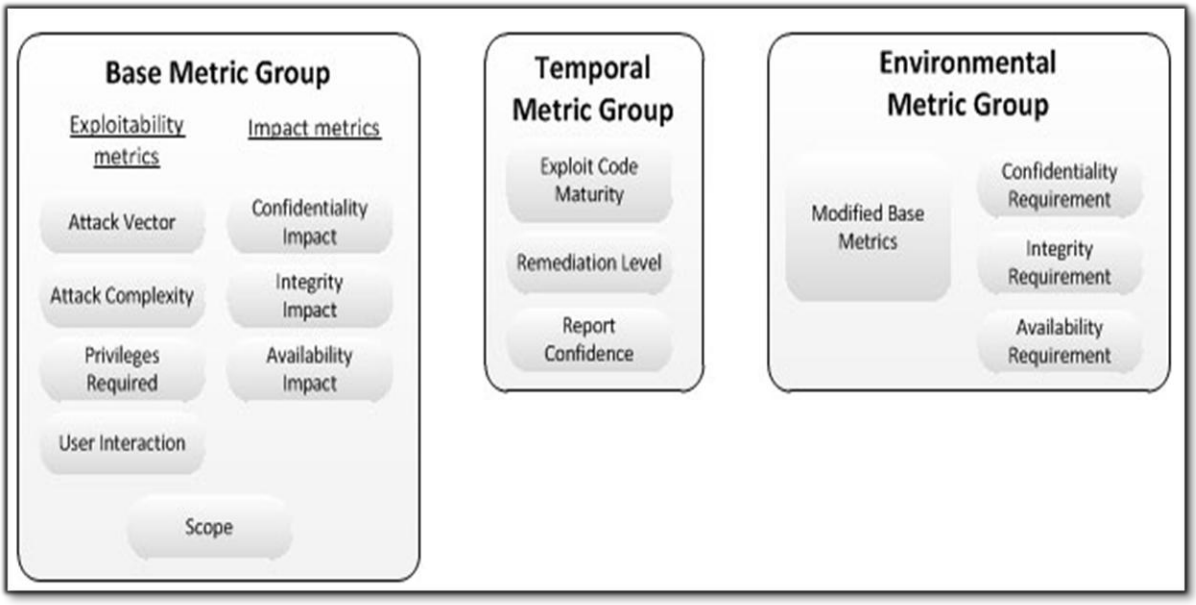
Como su término en inglés Common Vulnerability Scoring System, es un sistema diseñado para calificar o cuantificar por medio de un método abierto y estándar, el cual permite estimar el impacto de las vulnerabilidades identificadas en los sistemas de Información, permitiendo asignar la severidad de dichas vulnerabilidades.

Este sistema CVSS es administrado por *Forum of Incident Response and Security Teams* (FIRST), pero se trata de un estándar completamente abierto, por lo que puede ser utilizado libremente.

4.3 NIVELES DE CRITICIDAD DE VULNERABILIDADES EN LAS BASES DE DATOS PÚBLICAS

Existen varios niveles de criticidad que están categorizados según su probabilidad, facilidad, información, entre otros vectores. En la Figura 1 se visualiza como el CVSS v3.0 tiene los diferentes grupos de métricas, para poder asignar una criticidad a una vulnerabilidad. Las criticidades que asigna este estándar se detallan en el Cuadro 1.

Figura 1. CVSSv3 Grupos de métricas



Fuente. FIRST. Common Vulnerability Scoring System v3.0. Calculator. 1998. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <. https://www.first.org/cvss/calculator/3.0

Cuadro 1. Métricas de valoración de vulnerabilidades

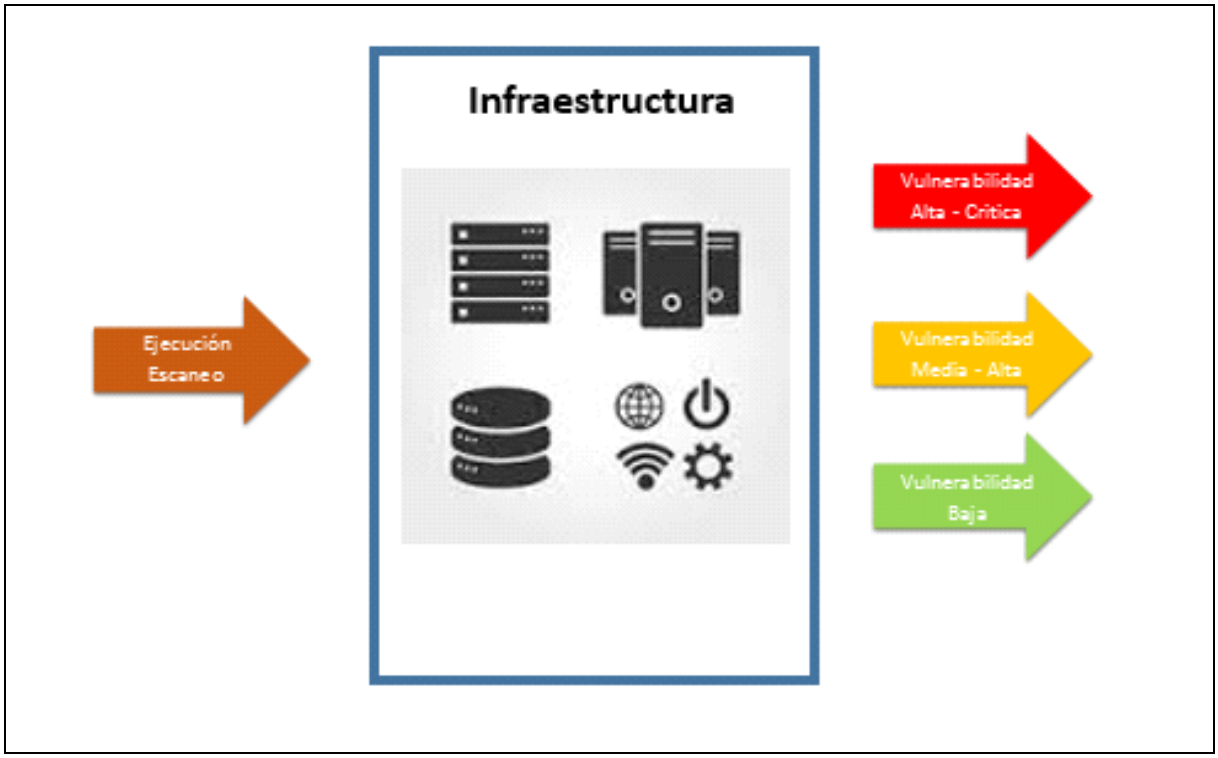
Criticidad	Valor
Crítico	9.0 a 10.0
Alto	7.0 a 8.9
Medio	4.0 a 6.9
Bajo	0.1 a 3.9

Fuente. FIRST. Common Vulnerability Scoring System v3.0. Calculator. 1998. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.first.org/cvss/calculator/3.0

4.4 TECNOLOGIAS PARA LA DETECCIÓN DE VULNERABILIDADES

Existen tecnologías desarrolladas por grandes fabricantes con el objetivo de poder identificar las vulnerabilidades en los sistemas operativos más reconocidos. Estas herramientas están diseñadas para detectar las vulnerabilidades por medio de firmas y proporcionan un informe en el cual detallan; el equipo donde se identificó la vulnerabilidad, su criticidad, referencias a posibles soluciones, entre otras.

Figura 2. Escaneo de vulnerabilidades y su criticidad



Fuente. Autores.

4.5 NORMATIVAS Y PRÁCTICAS LÍDERES QUE EXIGEN EL ESCANEO DE VULNERABILIDADES A ENTIDADES FINANCIERAS

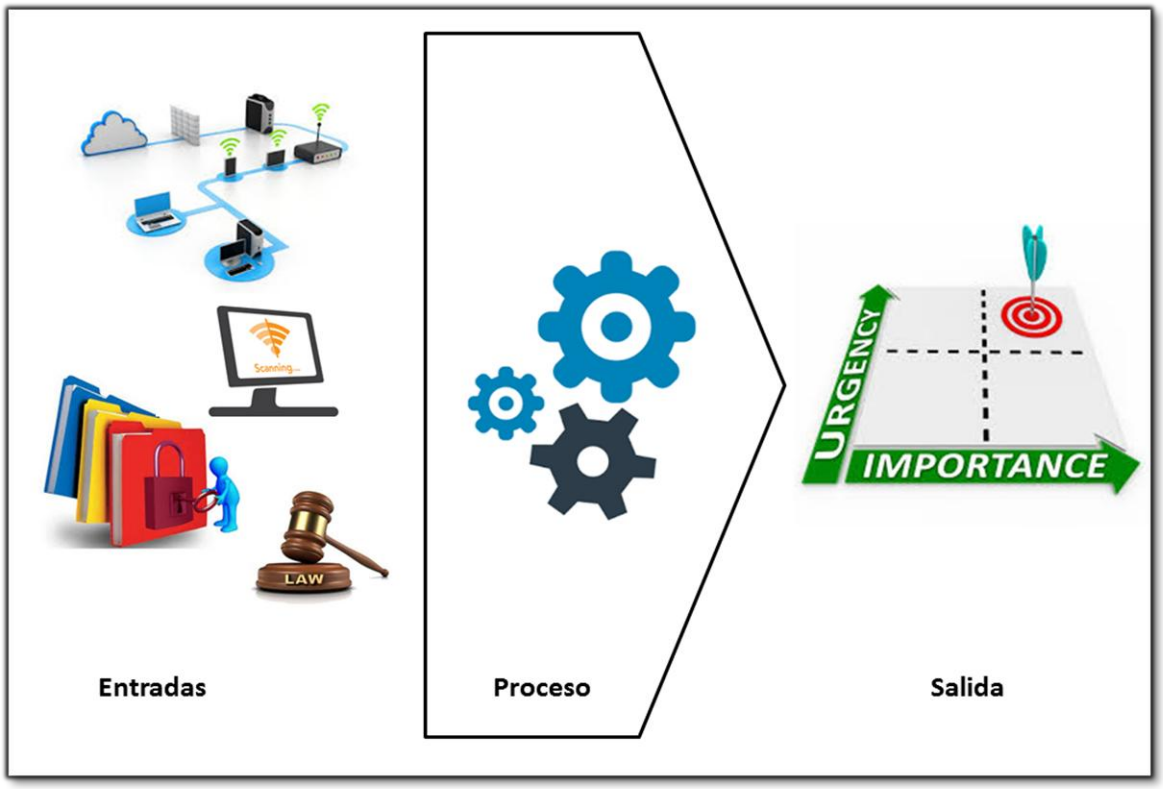
Dependiendo del objeto de negocio de las organizaciones colombianas, existen normativas y practicas líderes que exigen realizar escaneos en sus infraestructuras con ciertas frecuencias, el objetivo es evitar la explotación de las vulnerabilidades y una vez se tengan identificadas realizar la gestión para remediarlas. Las entidades del sector financiero las regula la superintendencia financiera de Colombia por medio de la circular 029 y también son supervisadas por las franquicias de tarjetas como Master Card y Visa mediante su norma Payment Card Industry (PCI[20]).

A pesar que esta última aun no es una norma de obligatorio cumplimiento es una práctica líder que se debe cumplir, la cual informa las mejores prácticas en el manejo de la información de los tarjetahabientes.

[20] PCI Industria de tarjetas de pago

Los informes de escaneos de vulnerabilidades son el único insumo que en la actualidad tiene Banco de Occidente, mediante estos inicia el proceso de remediación de vulnerabilidades, en el cual tienen en cuenta la categorización que le brindan las bases de datos públicas, anteriormente enunciadas con sus niveles de criticidad. Sin embargo, la infraestructura de la entidad va en crecimiento y su número de vulnerabilidades se multiplica dando como resultado un reporte inmanejable para las áreas de tecnología, las cuales son las directamente responsables en efectuar dicha gestión.

Figura 3. Identificación vulnerabilidades críticas para la entidad



Fuente. Autores

Teniendo en cuenta el panorama actual en la entidad, se pretende establecer una metodología para identificar las vulnerabilidades más críticas por medio de información obtenida del escaneo de vulnerabilidades, la infraestructura, normativas y el manejo de información sensible – Figura 3.

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Este proyecto está fundamentado en el modelo de investigación de tipo descriptiva.

5.2 HIPÓTESIS

5.2.1 Hipótesis inicial. La metodología propuesta identifica las vulnerabilidades que generan mayor riesgo en el Banco de Occidente.

5.2.2 Hipótesis nula. La identificación de vulnerabilidades críticas en el Banco de Occidente mediante la metodología propuesta no va a minimizar el riesgo.

5.3 VARIABLES

5.3.1 Variable independiente. Identificación de vulnerabilidades críticas.

5.3.2 Variable dependiente. Minimizar los riesgos de explotación de una vulnerabilidad.

5.4 TÉCNICAS PARA RECOLECCIÓN DE INFORMACIÓN

Para lograr evaluar la metodología propuesta e identificar si cumple con el objetivo, se utilizó las siguientes técnicas para obtener la información:

- Entrevistas,
- Métodos estadísticos.

5.4.1 Entrevistas. Se entrevistó a los administradores de las áreas de Tecnología e Infraestructura, con el objetivo de obtener las actividades y tiempos requeridos para la gestión de vulnerabilidades. Con la información recolectada se realizó tabulación por actividad con el fin de determinar los tiempos aproximados[21] y así evaluar si la metodología genera mejoras en los tiempos de gestión (Véase Anexo *A*)

[21] La respuesta de cada uno de los administradores se especificó en minutos y se generó un promedio el cual se utilizó para representar el tiempo de cada actividad. Cabe aclarar que la respuesta brindada por el administrador tiene un gran porcentaje de subjetividad debido que depende de la experiencia del mismo y la solución de la vulnerabilidad que varía entre una y otra.

Las áreas entrevistadas son las que hacen parte del comité que se realiza bimestralmente en la entidad y se relacionan en el Cuadro 2:

Cuadro 2. Áreas de TI que gestionan las vulnerabilidades

Área	Alcance	Filtro
Soporte Windows	Servidores con sistema operativo Windows	1
AIX / Linux	Servidores con sistema operativo AIX o Linux	1
Base de Datos	Bases de datos Oracle o MS SQL	1
Soporte a usuarios	Equipos de escritorio o portátiles	1
Telecomunicaciones	Switch o dispositivos de comunicación	1
Web	Servicios como apache, IIS, etc.	2
Aplicación	Proveedor de aplicación interna o externa	2

Fuente. Autores

Si la vulnerabilidad identificada no puede ser remediada por el ingeniero que se encuentra en el filtro 1, (filtro en el cual se da inicio a la gestión de las vulnerabilidades), esté escala el tema a áreas que pertenecen al filtro 2.

Debido a la infraestructura tecnológica de la entidad y segmentación en ambientes como son; productivo, pruebas y desarrollo, las actividades y tiempo para remediar las vulnerabilidades pueden diferir una a otra dependiendo donde fue identificada. En el Cuadro 3 se relacionan los tiempos de las actividades más relevantes y comunes entre las diferentes áreas relacionadas en el Cuadro 2, para gestionar las vulnerabilidades con los valores obtenidos en las entrevistas. Es importante mencionar que se clasificaron en tres grupos como se describen a continuación:

- Activos en ambiente productivo y hacen parte del Core de negocio: son los activos que son fundamentales en los procesos de la entidad.

- Activos en ambiente productivo y no hacen parte del Core: son aquellos activos que se encuentran en producción y son soporte para muchos procesos a la operación de la entidad.

- Activos que no están en ambiente productivo: son aquellos activos que se encuentran en los ambientes de pruebas y desarrollo.

Cuadro 3. Actividades y tiempos promedio para la gestión de vulnerabilidades

Activo de información	Actividades generales	Tiempo esfuerzo (min)
Si está en ambiente productivo y pertenece al Core de negocio	Validar la vulnerabilidad que si aplique a su plataforma	17
	Documentación sobre el problema que ocasiona la vulnerabilidad	67
	Generar un plan de acción para implementar la solución de la vulnerabilidad	55
	Generar control de cambios	52
	Aplicar la actualización o parche en ambiente de pruebas	53
	Validar si las pruebas no afectan la funcionalidad del activo de información para el objetivo de negocio (pruebas)	1029
	Generar control de cambios	52
	Aplicar la actualización en ambiente productivo	105
	Validar si no generan ningún tipo de indisponibilidad en el negocio	452
	TOTAL	**1895**
Si está en ambiente productivo y No pertenece al Core de negocio	Validar la vulnerabilidad que si aplique a su plataforma	17
	Documentación sobre el problema que ocasiona la vulnerabilidad	67
	Generar un plan de acción para implementar la solución de la vulnerabilidad	55
	Generar control de cambios	52
	Aplicar la actualización en ambiente productivo	105
	Validar si no generan ningún tipo de indisponibilidad en el negocio	452
	TOTAL	**748**
No está en ambiente productivo	Validar la vulnerabilidad que si aplique a su plataforma	17
	Documentación sobre el problema que ocasiona la vulnerabilidad	67
	Generar un plan de acción para implementar la solución de la vulnerabilidad	55
	Generar control de cambios	52
	Aplicar la actualización en ambiente de pruebas o desarrollo	53
	Validar si las pruebas no afectan la funcionalidad del activo de información para el objetivo de negocio (pruebas)	1029
	TOTAL	**1286**

Fuente. Autores

Nota: Es importante aclarar que los tiempos intermedios entre algunas de las actividades, como son la periodicidad del comité de control de cambios o validación de aplicaciones por el área de calidad, no se tiene en cuenta debido a la gran variabilidad de estos.

5.4.2 Métodos estadísticos. Esta investigación está basada con datos de prueba para evaluar un porcentaje de equipos de la entidad que representan el 10% de los activos de información a nivel de servidores que soportan los servicios. Este porcentaje de equipos tiene componentes como (Véase Anexo *B*):

- Activos de información de diferentes ambientes de la entidad (productivo, pruebas, desarrollo).
- Activos de información con diferente valor para la entidad (mayor riesgo - clasificación de activos de información).
- Activos de información ubicados en diferentes segmentos de la red de telecomunicaciones (ubicación física en la red).
- Activos de información con diferentes sistemas operativos.
- Rol en el negocio (aplicación, plataforma, BD, etc.).

Cuadro 4. Activos evaluados

Ítem	Cantidad
Total Activos de información	70
Ambiente productivo	28
Ambiente de pruebas	21
Ambiente de desarrollo	21
Aplicación Core	7

Fuente. Autores

Este trabajo se focaliza en aplicar la metodología en las vulnerabilidades identificadas en servidores, teniendo en cuenta el alto impacto que representan para la entidad, sin embargo, la metodología propuesta también puede aplicarse para equipos de usuario o escritorio.

6. DESARROLLO

6.1 GENERALIDADES

El Banco de Occidente ejecuta un escaneo al total de la infraestructura como máximo cada 6 meses con el objetivo de cumplir con normativas que exigen realizar esta actividad, mencionado anteriormente circular 029 emitida por la Superintendencia Financiera de Colombia. El resultado o producto de dicha actividad es un informe con las vulnerabilidades identificadas, clasificadas por su nivel de criticidad. En el cuadro 5 se relacionan los tiempos definidos por el área de seguridad de la información de la entidad, para gestionar las vulnerabilidades según su criticidad.

Cuadro 5. Tiempos definidos para el cierre de vulnerabilidades según su criticidad

Criticidad	Tiempo
Alta	30 días
Media	60 días
Baja	90 días

Fuente. Autores

Nota: Las vulnerabilidades identificadas como críticas, la entidad las consolida con las altas.

6.2 DATOS ESCANEO

La cantidad de vulnerabilidades identificadas por criticidad, se relacionan en el cuadro 6 (Véase Anexo *C*):

Cuadro 6. Número de vulnerabilidades por criticidad

Criticidad	Cantidad Vulnerabilidades
Criticas	145
Altas	57
Medias	126
Bajas	54
Total	**382**

Fuente. Autores

Nota: Las vulnerabilidades identificadas por la herramienta Como "Informativas", se excluyen de la gestión.

En el Cuadro 7 complementa el Cuadro 6, en el cual se relaciona la cantidad de vulnerabilidades especificando su criticidad y ambiente del activo de información donde fue identificada, obteniendo los siguientes datos:

Cuadro 7. Cantidad de vulnerabilidades por ambiente

Criticidad	Cantidad Vulnerabilidades	Ambiente Productivo + Core	Ambiente Productivo No Core	Ambiente de pruebas o desarrollo
Criticas	145	11	48	86
Altas	57	7	15	35
Medias	126	11	37	78
Bajas	54	5	17	32
Total	**382**	**34**	**117**	**231**

Fuente. Autores

Tenido presente la información anteriormente descrita se procede a dar una descripción de la metodología utilizada actualmente.

6.3 ESCENARIO 1 – METODOLOGÍA ACTUAL

El criterio para gestionar las vulnerabilidades en Banco de Occidente tiene el siguiente orden (Véase Anexo D):

1. Críticas en ambiente productivo más Core,
2. Altas en ambiente productivo más Core,
3. Medias en ambiente productivo más Core,
4. Críticas en ambiente productivo no Core,
5. Altas en ambiente productivo no Core,
6. Medias en ambiente productivo no Core,
7. Críticas en ambiente de pruebas y desarrollo,
8. Altas en ambiente de pruebas y desarrollo,
9. Medias en ambiente de pruebas y desarrollo.

Debido al gran volumen, las vulnerabilidades de criticidad baja por el momento no se están gestionando (Véase Anexo E).

En el Cuadro 8 se estiman los tiempos de gestión de las vulnerabilidades identificadas, presentando el valor total del esfuerzo (en días), su criticidad y ambiente. Es importante aclarar que el valor generado está contemplado como un dato global y no se tiene en cuenta la cantidad de personas que están asignadas por cada área para llevar a cabo dicha labor.

Cuadro 8. Esfuerzo en tiempo para la gestión de vulnerabilidades por criticidad y ambiente en escenario 1.

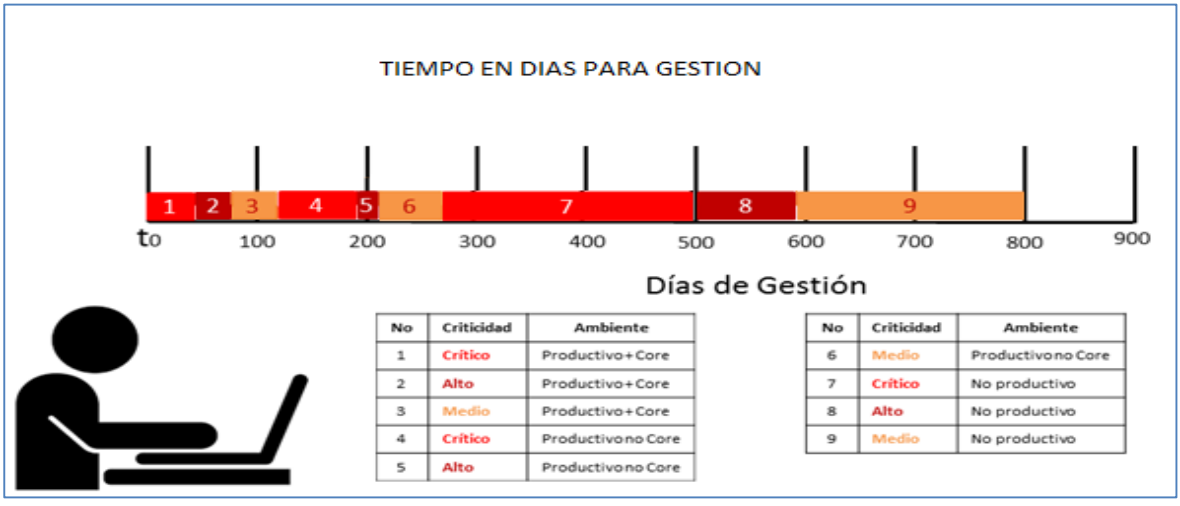
Criticidad	Cantidad Vulnerabilidades	Ambiente Productivo + Core	Esfuerzo (min) 1895	Ambiente Productivo No Core	Esfuerzo (min) 748	Ambiente de Pruebas	Esfuerzo (min) 1286	Esfuerzo TOTAL Minutos	Esfuerzo TOTAL HORAS	Esfuerzo TOTAL Días
Criticas	145	11	20845	48	35904	86	110596	167345	2789,1	348,6
Altas	57	7	13265	15	11220	35	45010	69495	1158,3	144,8
Medias	126	11	20845	37	27676	78	100308	148829	2480,5	310,1
	328	**29**		**100**		**199**		**385669,0**	**6427,8**	**803,5**

Fuente. Autores

En la Gráfica 2, se ubica en orden las vulnerabilidades que se gestionan en este escenario y se identifican las siguientes desventajas:

- La entidad no tiene un panorama completo de las vulnerabilidades que puedan afectar activos críticos.
- No existe un orden específico de las vulnerabilidades a gestionar por criticidad, lo que conlleva a que el administrador de plataforma gestione subjetivamente sin evaluar el mayor grado de exposición de la entidad.
- El tiempo de exposición de la entidad es muy amplio para gestionar vulnerabilidades críticas y altas (véase la Grafica 2).
- Coexistir por tiempos muy largos con un nivel de exposición alto, al no identificar las vulnerabilidades con mayor impacto, son tiempos que pueden ser aprovechados por un atacante (véase la Grafica 3).

Gráfica 2. Tiempo de gestión de vulnerabilidades según su criticidad y ambiente



No	Criticidad	Ambiente
1	Crítico	Productivo+Core
2	Alto	Productivo+Core
3	Medio	Productivo+Core
4	Crítico	Productivo no Core
5	Alto	Productivo no Core

No	Criticidad	Ambiente
6	Medio	Productivo no Core
7	Crítico	No productivo
8	Alto	No productivo
9	Medio	No productivo

Fuente. Autores

Gráfica 3. Nivel de exposición[22] aproximado con metodología actual

Fuente. Autores

Presentada la metodología utilizada en la actualidad, se procede a describir la metodología propuesta.

6.4 ESCENARIO 2- METODOLOGIA PROPUESTA

A continuación, se explica cada uno de los componentes y pasos esenciales para aplicar la metodología propuesta. Los valores numéricos fueron obtenidos de diferentes pruebas realizadas, donde se confirmó que al seleccionar números con intervalos para cada una de las escalas (ejemplo: tipo de información, normativas, criticidad de vulnerabilidades, entre otras) se adaptan mejor a la metodología al dejar vacíos de manera que al realizar las operaciones se adhiera mejor al análisis a evaluar y determinar el orden de atención o priorización de la vulnerabilidad.

Los siguientes pasos son requeridos para la metodología propuesta a evaluar:

6.4.1 Valoración de activos por tipo de información y normativas. Se genera clasificación de activos de información, teniendo en cuenta los tipos de información que maneja la entidad, la cual debe velar por conservar la confidencialidad, integridad o disponibilidad requerida y las diferentes normativas o practicas líderes que en la actualidad se exige a las entidades del sector financiero, mencionadas con anteriorid ad (029 SFC, PCI). Para lograr adaptar

[22] Nivel de Exposición: Tiempo durante el cual se encuentra presente las vulnerabilidades en las plataformas.

estos datos a la metodología propuesta, se asignan valores numéricos a los diferentes criterios como se observa en el Cuadro 9.

Tabla 9. Valoración numérica para los tipos de información y normatividad

Criterios	Explicación	Valor Descriptivo	Valor Numérico
Tipo de información	Depende del tipo de información que contiene o maneja el activo de información	Restringida	9
		Confidencial	7
		Interna	5
		Publica	3
Normatividad	Leyes, normativas o circulares que obliga o genera las mejores prácticas para el manejo de información bancaria	SOX	9
		Circular 029	9
		PCI	7
		No aplica ninguna normatividad	1

Fuente. Autores

Con la información del Cuadro 9 se genera la valoración del Cuadro 10, para calcular numéricamente los activos de información teniendo en cuenta los criterios de tipo de información y normatividad dando como resultado una nueva valoración (Véase Cuadro 10).

Cuadro 10. Valoración numérica por tipo de información vs normatividad

Tipo de información	Normatividad	Valoración
9	9	9
7	9	9
9	6	8
9	1	8
7	1	8
7	6	8
5	9	7
5	6	5
3	9	4
3	6	3
5	1	2
3	1	1

Fuente. Autores

6.4.2 Valoración criticidad vulnerabilidades. Para las criticidades de las vulnerabilidades, utilizadas por la herramienta de escaneo relacionadas en el cuadro 6, se hace necesario generar una escala de valores como se presenta en el Cuadro 11.

Cuadro 11. Valoración numérica para las criticidades de las vulnerabilidades

Criticidad	Valor
Critica	9
Alto	7
Medio	5
Bajo	3

Fuente. Autores

En la ecuación 1 se toman los criterios anteriormente descritos; valor de criticidad de la vulnerabilidad por la sumatoria del valor de la normativa y sí es core se suma 9.

Ecuación 1

$$\boldsymbol{Score\ 1} = Valor\ Crit.Vulnera. \times (Valor\ de\ Normativa\ vs\ Tipo\ de\ Info. + Valor\ Core)$$

6.4.3 Valoración de Activos por zonas. El Banco de Occidente controla el tráfico de red entre segmentos mediante el firewall[23] separando por zonas[24], por tal motivo para lograr una valoración del nivel de exposición de los activos (equipo, servidor, etc.) en una red, se debe tener en cuenta que hay activos que comparten zonas y el riesgo al que pueden verse expuestos puede ser mayor al reportado en el informe generado por el escáner de vulnerabilidades, por ejemplo, si en una misma zona de red se encuentran dos activos, uno de ellos maneja información sensible core de la entidad, esté presenta una vulnerabilidad clasificada como baja; el segundo un activo el cual maneja información de carácter público, y no hace parte de los activos core de la entidad, sin embargo esté, cuenta con una vulnerabilidad de criticidad critica; este escenario hace que al segundo activo se le deba cambiar su prioridad en la valoración y gestión.

A continuación se especifican las zonas que se encuentran en el Banco de Occidente (Ver Cuadro 12).

[23] Firewall parte de un sistema o dispositivo de seguridad perimetral que controla los accesos, el cual se permite o deniega el acceso a determinados segmentos de red.

[24] Zona Segmentación realizada por el Firewall

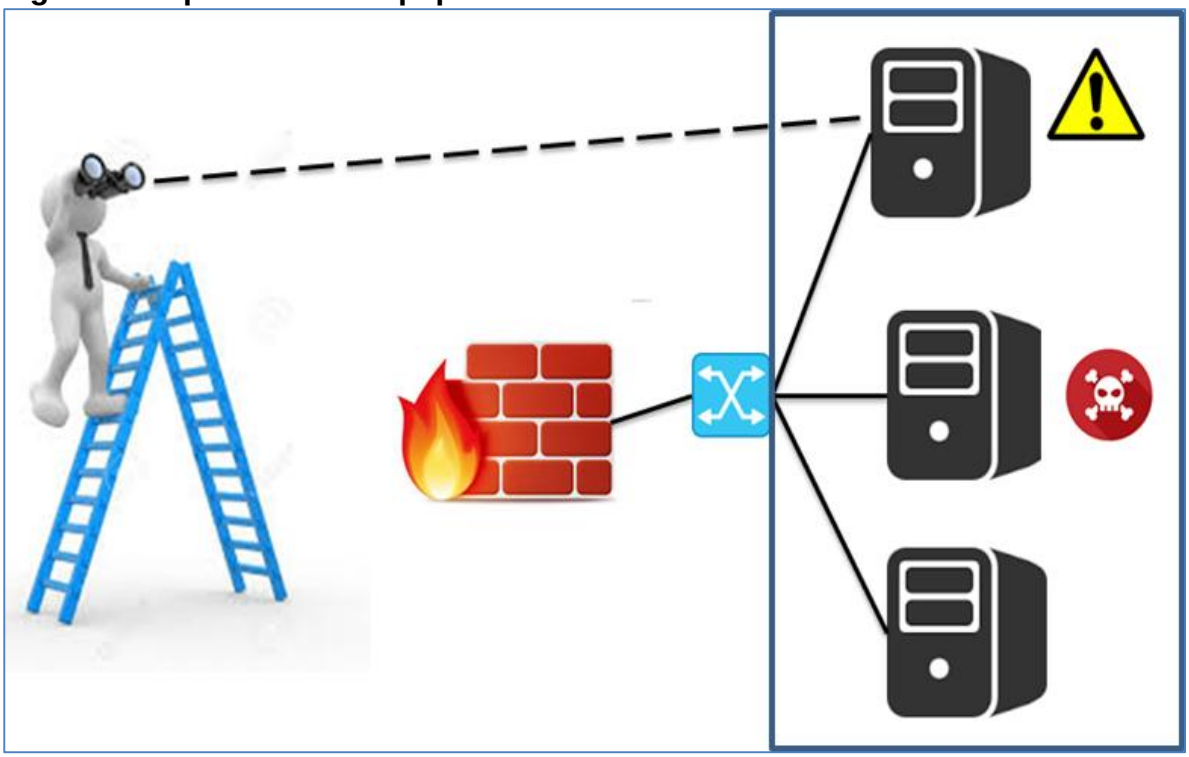
6.4.4 Zonas existentes

Cuadro 12. Existentes

ZONA
Servidores Productivo
Servidores Pruebas y Desarrollo
DMZ Producción
DMZ Pruebas
PCs Tesoreria
PCs STAFF

Fuente. Autores

Figura 4. Exposición de equipos en una red local virtual



Fuente. Autores

El insumo para poder generar la valoración por zona se obtiene del área de telecomunicaciones, con el cual se identifican los segmentos de red asignándoles un identificador (Véase Anexo F y G).

En la metodología propuesta se valora la criticidad de las vulnerabilidades de los activos, no solo por las identificadas en el mismo, sino también por las de su entorno. Para ello se utilizan las siguientes formulas.

Con las ecuaciones 2,3, 4 y 5 tienen como objetivo generar un valor de score teniendo en cuenta la cantidad de vulnerabilidades por la criticidad en cada una de las zonas.
En la ecuación 2

Ecuación 2:

$$\boldsymbol{Score\ por\ Criticidad\ Vulnerabilidades\ Criticas\ por\ Zona} = Cantidad\ de\ Vulnerabilidades\ Criticas\ por\ zona\ X\ 7$$

En la ecuación 3

Ecuación 3: $$\boldsymbol{Score\ por\ Criticidad\ Vulnerabilidades\ Alta\ por\ Zona} = Cantidad\ de\ Vulnerabilidades\ Altas\ por\ zona\ X\ 7$$

En la ecuación 4

Ecuación 4

$$\boldsymbol{Score\ por\ Criticidad\ Vulnerabilidades\ Media\ por\ Zona} = Cantidad\ de\ Vulnerabilidades\ Medias\ por\ zona\ X\ 5$$

En la ecuación 5

Ecuación 5

$$\boldsymbol{Score\ por\ Criticidad\ Vulnerabilidades\ Bajas\ por\ Zona} = Cantidad\ de\ Vulnerabilidades\ Bajas\ por\ zona\ X\ 3$$

En la ecuación 6 busca obtener un score del nivel de riesgo con la sumatoria de las vulnerabilidades por cada zona, teniendo en cuenta la cantidad de activos en la misma.

Ecuación 6

$$\boldsymbol{Ponderado\ Total\ Criticidad\ por\ Zona} = \frac{\sum Score\ por\ Criticidad\ (Alto, Medio\ y\ Bajo) por\ zona}{Cantidd\ de\ Activos\ por\ zona}$$

En la ecuación 7 se suma el resultado de las ecuaciones número .1 (Score 1) más la ecuación número 6 (Ponderado Total Criticidad por Zona), dando como resultado el nuevo valor de la criticidad por zona.

Ecuación 7

$$\boldsymbol{Score\ Total = Score\ 1 + Ponderado\ Total\ Criticidad\ por\ Zona}$$

6.5 APLIACIÓN DE LA METODOLOGÍA

Para mayor comprensión de cómo se cuantifican cada uno de los valores explicados anteriormente, se toma el siguiente ejemplo de un escaneo. La muestra es de 15 equipos que se relacionan las direcciones IP el Cuadro 13, donde se identifican 14 vulnerabilidades relacionadas en el Cuadro 14.

Cuadro 13. Equipos escaneados

Equipos
192.168.1.11
192.168.1.12
192.168.1.15
192.168.1.18
192.168.1.2
192.168.1.5
192.168.1.7
192.168.1.9
192.168.2.10
192.168.2.13
192.168.2.14
192.168.2.16
192.168.2.3
192.168.2.4
192.168.2.6

Fuente. Autores

Cuadro 14. Vulnerabilidades identificadas

Vulnerabilidad	Criticidad
P	Critico
B	Critico
V	Critico
A	Alto
H	Medio
M	Alto
S	Bajo
T	Bajo
U	Medio
I	Critico
L	Medio
E	Bajo
C	Critico
D	Alto
Q	Bajo

Fuente. Autores

Se tienen un total de 23 vulnerabilidades debido a que un equipo puede tener n vulnerabilidades, como se puede observar en el Cuadro 15.

Cuadro 15. Total de vulnerabilidades

IP	Vulnerabilidad	Criticidad
192.168.1.2	P	CRITICO
192.168.2.14	B	CRITICO
192.168.2.4	V	CRITICO
192.168.1.5	A	ALTO
192.168.1.5	B	CRITICO
192.168.2.4	H	MEDIO
192.168.2.13	M	ALTO
192.168.1.2	S	BAJO
192.168.1.7	T	BAJO
192.168.1.5	U	MEDIO
192.168.1.5	T	BAJO
192.168.1.18	P	CRITICO
192.168.2.3	P	CRITICO
192.168.2.6	I	CRITICO
192.168.1.11	L	MEDIO
192.168.1.15	E	BAJO
192.168.1.15	S	BAJO
198.168.1.12	C	CRITICO
192.168.1.18	D	ALTO
192.168.1.9	L	MEDIO
192.168.2.10	T	BAJO
192.168.2.16	U	MEDIO
192.168.2.16	Q	BAJO

Fuente. Autores

Para aplicar la metodología, en el Cuadro 16 se asigna el valor numérico a cada una de las criticidades de las vulnerabilidades como se explicó anteriormente en el Cuadro 11.

Cuadro 16. Asignación de valor numérico a las vulnerabilidades

IP	Vulnerabilidad	Criticidad	Criticidad Vulnerabilidad
192.168.1.2	P	CRITICO	9
192.168.2.14	B	CRITICO	9
192.168.2.4	V	CRITICO	9
192.168.1.5	A	ALTO	7
192.168.1.5	B	CRITICO	9
192.168.2.4	H	MEDIO	5
192.168.2.13	M	ALTO	7
192.168.1.2	S	BAJO	3
192.168.1.7	T	BAJO	3
192.168.1.5	U	MEDIO	5
192.168.1.5	T	BAJO	3
192.168.1.18	P	CRITICO	9
192.168.2.3	P	CRITICO	9
192.168.2.6	I	CRITICO	9
192.168.1.11	L	MEDIO	5
192.168.1.15	E	BAJO	3
192.168.1.15	S	BAJO	3
198.168.1.12	C	CRITICO	9
192.168.1.18	D	ALTO	7
192.168.1.9	L	MEDIO	5
192.168.2.10	T	BAJO	3
192.168.2.16	U	MEDIO	5
192.168.2.16	Q	BAJO	3

Fuente. Autores

Posteriormente se identifica cada activo mediante su dirección (IP) al ambiente que pertenece en la infraestructura tecnológica, si es Core y que tipo de información maneja como se observa en el Cuadro 17.

Cuadro 17. Identificación de activos, dirección IP, tipo de información

IP	Ambiente	Core	Tipo de Información
192.168.1.2	Productivo	Si	Restringida
192.168.2.14	Productivo	Si	Restringida
192.168.2.4	Productivo	Si	Confidencial
192.168.1.5	Productivo	Si	Restringida
192.168.1.5	Productivo	No	Confidencial
192.168.2.4	Productivo	Si	Confidencial
192.168.2.13	Productivo	No	Iinterna
192.168.1.2	Productivo	Si	Restringida
192.168.1.7	Productivo	Si	Confidencial
192.168.1.5	Productivo	No	Confidencial
192.168.1.5	Productivo	No	Confidencial
192.168.1.18	Desarrollo	No	Iinterna
192.168.2.3	Pruebas	No	Iinterna
192.168.2.6	Desarrollo	No	Iinterna
192.168.1.11	Productivo	No	Publica
192.168.1.15	Productivo	No	Iinterna
192.168.1.15	Productivo	No	Iinterna
198.168.1.12	Productivo	No	Iinterna
192.168.1.18	Desarrollo	No	Iinterna
192.168.1.9	Desarrollo	No	Iinterna
192.168.2.10	Pruebas	No	Iinterna
192.168.2.16	Pruebas	No	Publica
192.168.2.16	Pruebas	No	Publica

Fuente. Autores

En el Cuadro 18 se asignan los valores según el tipo de información que maneja el activo como se explicó anteriormente en el Cuadro 9.

Cuadro 18. Valores tipo de información

IP	Ambiente	Core	Tipo de Información	Valor de Información
192.168.1.2	Productivo	Si	Restringida	9
192.168.2.14	Productivo	Si	Restringida	9
192.168.2.4	Productivo	Si	Confidencial	7
192.168.1.5	Productivo	Si	Restringida	9
192.168.1.5	Productivo	No	Confidencial	7
192.168.2.4	Productivo	Si	Confidencial	7
192.168.2.13	Productivo	No	Iinterna	5
192.168.1.2	Productivo	Si	Restringida	9
192.168.1.7	Productivo	Si	Confidencial	7
192.168.1.5	Productivo	No	Confidencial	7
192.168.1.5	Productivo	No	Confidencial	7
192.168.1.18	Desarrollo	No	Iinterna	5
192.168.2.3	Pruebas	No	Iinterna	5
192.168.2.6	Desarrollo	No	Iinterna	5
192.168.1.11	Productivo	No	Publica	3
192.168.1.15	Productivo	No	Iinterna	5
192.168.1.15	Productivo	No	Iinterna	5
198.168.1.12	Productivo	No	Iinterna	5
192.168.1.18	Desarrollo	No	Iinterna	5
192.168.1.9	Desarrollo	No	Iinterna	5
192.168.2.10	Pruebas	No	Iinterna	5
192.168.2.16	Pruebas	No	Publica	3
192.168.2.16	Pruebas	No	Publica	3

Fuente. Autores

En el Cuadro 19 se identifica para cada activo si aplica alguna normatividad como SOX, CSF029, PCI o no aplica ninguna.

Cuadro 19. Activos por normativa

IP	Ambiente	Core	Normatividad
192.168.1.2	Productivo	Si	SOX
192.168.2.14	Productivo	Si	CSF 042
192.168.2.4	Productivo	Si	CSF 042
192.168.1.5	Productivo	Si	SOX
192.168.1.5	Productivo	No	PCI
192.168.2.4	Productivo	Si	CSF 042
192.168.2.13	Productivo	No	SOX
192.168.1.2	Productivo	Si	SOX
192.168.1.7	Productivo	Si	CSF 042
192.168.1.5	Productivo	No	PCI
192.168.1.5	Productivo	No	PCI
192.168.1.18	Desarrollo	No	NA
192.168.2.3	Pruebas	No	NA
192.168.2.6	Desarrollo	No	NA
192.168.1.11	Productivo	No	PCI
192.168.1.15	Productivo	No	PCI
192.168.1.15	Productivo	No	PCI
198.168.1.12	Productivo	No	NA
192.168.1.18	Desarrollo	No	NA
192.168.1.9	Desarrollo	No	NA
192.168.2.10	Pruebas	No	NA
192.168.2.16	Pruebas	No	NA
192.168.2.16	Pruebas	No	NA

Fuente. Autores

En el Cuadro 20 se procede a asignar los valores por normatividad, teniendo en cuenta el cuadro 9 visto anteriormente.

Cuadro 20. Cuantificación de las normativas

IP	Ambiente	Core	Normatividad	Valor Normatividad
192.168.1.2	Productivo	Si	SOX	9
192.168.2.14	Productivo	Si	CSF 042	9
192.168.2.4	Productivo	Si	CSF 042	9
192.168.1.5	Productivo	Si	SOX	9
192.168.1.5	Productivo	No	PCI	7
192.168.2.4	Productivo	Si	CSF 042	9
192.168.2.13	Productivo	No	SOX	9
192.168.1.2	Productivo	Si	SOX	9
192.168.1.7	Productivo	Si	CSF 042	9
192.168.1.5	Productivo	No	PCI	7
192.168.1.5	Productivo	No	PCI	7
192.168.1.18	Desarrollo	No	NA	1
192.168.2.3	Pruebas	No	NA	1
192.168.2.6	Desarrollo	No	NA	1
192.168.1.11	Productivo	No	PCI	7
192.168.1.15	Productivo	No	PCI	7
192.168.1.15	Productivo	No	PCI	7
198.168.1.12	Productivo	No	NA	1
192.168.1.18	Desarrollo	No	NA	1
192.168.1.9	Desarrollo	No	NA	1
192.168.2.10	Pruebas	No	NA	1
192.168.2.16	Pruebas	No	NA	1
192.168.2.16	Pruebas	No	NA	1

Fuente. Autores

Ahora en el Cuadro 21 se asigna la valoración vista anteriormente en el cuadro 10 con los resultados del tipo de información y normatividad, del cuadro 18 y 20 respectivamente.

Cuadro 21. Valoración activos tipo de información, normativa

IP	Ambiente	Core	Tipo de Información	Valor Tipo Información	Normatividad	Valor Normatividad	Valoracion Activo
192.168.1.2	Productivo	Si	Restringida	9	SOX	9	9
192.168.2.14	Productivo	Si	Restringida	9	CSF 042	9	9
192.168.2.4	Productivo	Si	Confidencial	7	CSF 042	9	9
192.168.1.2	Productivo	Si	Restringida	9	SOX	9	9
192.168.1.5	Productivo	No	Confidencial	7	PCI	7	7
192.168.2.4	Productivo	Si	Confidencial	7	CSF 042	9	9
192.168.2.13	Productivo	No	Iinterna	5	SOX	9	6
192.168.1.2	Productivo	Si	Restringida	9	SOX	9	9
192.168.1.7	Productivo	Si	Confidencial	7	CSF 042	9	9
192.168.1.5	Productivo	No	Confidencial	7	PCI	7	7
192.168.1.5	Productivo	No	Confidencial	7	PCI	7	7
192.168.1.18	Desarrollo	No	Iinterna	5	NA	1	2
192.168.2.3	Pruebas	No	Iinterna	5	NA	1	2
192.168.2.6	Desarrollo	No	Iinterna	5	NA	1	2
192.168.1.11	Productivo	No	Publica	3	PCI	7	3
192.168.1.15	Productivo	No	Iinterna	5	PCI	7	5
192.168.1.15	Productivo	No	Iinterna	5	PCI	7	5
198.168.1.12	Productivo	No	Iinterna	5	NA	1	2
192.168.1.18	Desarrollo	No	Iinterna	5	NA	1	2
192.168.1.9	Desarrollo	No	Iinterna	5	NA	1	2
192.168.2.10	Pruebas	No	Iinterna	5	NA	1	2
192.168.2.16	Pruebas	No	Publica	3	NA	1	1
192.168.2.16	Pruebas	No	Publica	3	NA	1	1

Fuente. Autores

Teniendo presente que ya se obtuvo el valor de la criticidad de la vulnerabilidad (Cuadro 16) y la valoración del activo (Cuadro 21), se multiplican estos dos valores, como se ilustra en el Cuadro 22, generando el primer valor al score[25], con ello se puede determinar que se priorizan los activos de acuerdo con normativa y clasificación de acceso a la información que contienen.

Cuadro 22. Valor Score por activo

IP	Tipo de Información	Normatividad	Valoración Activo	Vulnerabilidad	Criticidad	Valor Criticidad Vulnerabilidad	Score
192.168.1.2	Restringida	SOX	9	P	CRITICO	9	81
192.168.2.14	Restringida	CSF 042	9	B	CRITICO	9	81
192.168.2.4	Confidencial	CSF 042	9	V	CRITICO	9	81
192.168.1.2	Restringida	SOX	9	A	ALTO	7	63
192.168.1.5	Confidencial	PCI	7	B	CRITICO	9	63
192.168.2.4	Confidencial	CSF 042	9	H	MEDIO	5	45
192.168.2.13	Iinterna	SOX	6	M	ALTO	7	42
192.168.1.2	Restringida	SOX	9	S	BAJO	3	27
192.168.1.7	Confidencial	CSF 042	9	T	BAJO	3	27
192.168.1.5	Confidencial	PCI	7	U	MEDIO	5	35
192.168.1.5	Confidencial	PCI	7	T	BAJO	3	21
192.168.1.18	Iinterna	NA	2	P	CRITICO	9	18
192.168.2.3	Iinterna	NA	2	P	CRITICO	9	18
192.168.2.6	Iinterna	NA	2	I	CRITICO	9	18
192.168.1.11	Publica	PCI	3	L	MEDIO	5	15
192.168.1.15	Iinterna	PCI	5	E	BAJO	3	15
192.168.1.15	Iinterna	PCI	5	S	BAJO	3	15
198.168.1.12	Iinterna	NA	2	C	CRITICO	9	18
192.168.1.18	Iinterna	NA	2	D	ALTO	7	14
192.168.1.9	Iinterna	NA	2	L	MEDIO	5	10
192.168.2.10	Iinterna	NA	2	T	BAJO	3	6
192.168.2.16	Publica	NA	1	U	MEDIO	5	5
192.168.2.16	Publica	NA	1	Q	BAJO	3	3

Fuente. Autores

[25] Valor a la criticidad de la vulnerabilidad en la metodología propuesta

Una vez se obtiene el valor del score, ilustrado en el Cuadro 22, se le suma 9 en el caso que el activo pertenezca al Core de la Entidad, como se observa en el Cuadro 23, es importante resaltar que para los activos que no son Core no se suma ningún valor, esté conservar el valor asignado en el Cuadro 22, obteniendo el valor de la ecuación 1.

Cuadro 23. Valor nuevo score activo

IP	Ambiente	Core	Valor Core	Score	Nuevo Score
192.168.1.2	Productivo	Si	9	81	90
192.168.2.14	Productivo	Si	9	81	90
192.168.2.4	Productivo	Si	9	81	90
192.168.1.2	Productivo	Si	9	63	72
192.168.1.5	Productivo	No	0	63	63
192.168.2.4	Productivo	Si	9	45	54
192.168.2.13	Productivo	No	0	42	42
192.168.1.2	Productivo	Si	9	27	36
192.168.1.7	Productivo	Si	9	27	36
192.168.1.5	Productivo	No	0	35	35
192.168.1.5	Productivo	No	0	21	21
192.168.1.18	Desarrollo	No	0	18	18
192.168.2.3	Pruebas	No	0	18	18
192.168.2.6	Desarrollo	No	0	18	18
192.168.1.11	Productivo	No	0	15	15
192.168.1.15	Productivo	No	0	15	15
192.168.1.15	Productivo	No	0	15	15
192.168.1.12	Productivo	No	0	18	18
192.168.1.18	Desarrollo	No	0	14	14
192.168.1.9	Desarrollo	No	0	10	10
192.168.2.10	Desarrollo	No	0	6	6
192.168.2.16	Pruebas	No	0	5	5
192.168.2.16	Pruebas	No	0	3	3

Fuente. Autores

Posteriormente se identifican las zonas a las que pertenecen los activos de información, como se ilustra en el Cuadro 24.

Cuadro 24. Identificación de sub redes

IP	Zona
192.168.1.11	1
192.168.1.12	2
192.168.1.15	2
192.168.1.18	1
192.168.1.2	1
192.168.1.5	1
192.168.1.7	3
192.168.1.9	3
192.168.2.10	4
192.168.2.13	4
192.168.2.14	4
192.168.2.16	3
192.168.2.3	2
192.168.2.4	2
192.168.2.6	1

Fuente. Autores

Se procede a identificar por zonas las vulnerabilidades según su criticidad, como se ilustra en el Cuadro 25

Cuadro 25. Identificación de vulnerabilidades mayores o iguales a 7

IP	Zona	Valoración Criticidad Vullnerabilidad
192.168.1.18	1	9
192.168.1.2	1	9
192.168.1.5	1	9
192.168.2.6	1	9
192.168.1.18	1	7
192.168.1.2	1	7
192.168.1.11	1	5
192.168.1.5	1	5
192.168.1.2	1	3
192.168.1.5	1	3
192.168.1.12	2	9
192.168.2.3	2	9
192.168.2.4	2	9
192.168.2.4	2	5
192.168.1.15	2	3
192.168.1.15	2	3
192.168.1.9	3	5
192.168.2.16	3	5
192.168.1.7	3	3
192.168.2.16	3	3
192.168.2.14	4	9
192.168.2.13	4	7
192.168.2.10	4	3

Fuente. Autores

Como resultado de la identificación del Cuadro 25, se obtiene el Cuadro 26 en el cual se identifica por zona cuantas vulnerabilidades hay con valores mayores o iguales a 7 (Alta), iguales 5 (Medio) e iguales a 3 (Bajo) y se multiplica por el valor de la criticidad.

Cuadro 26. Identificación de vulnerabilidades por zonas

Zonas	Alta		Media		Baja	
	7		5		3	
1	6	42	2	10	2	6
2	3	21	1	5	2	6
3	0	0	2	10	3	9
4	1	7	0	0	1	3

Fuente. Autores

Consecutivamente se procede a totalizar el valor generado por cada zona en cada una de las criticidades, como se puede observar en el Cuadro 27.

Cuadro 27. Total vulnerabilidades por zona

Zonas	Alta		Media		Baja		Score Criticidad Vulnerabilidades
	7		5		3		
1	6	42	2	10	2	6	58
2	3	21	1	5	2	6	32
3	0	0	2	10	3	9	19
4	1	7	0	0	1	3	10

Fuente. Autores

Posteriormente se identifican el número de activos que tiene cada zona, como lo ilustra el Cuadro 28.

Cuadro 28. Número activos por zona

Zonas	Cantidad de Activos por Zona
1	5
2	4
3	3
4	3

Fuente. Autores

Teniendo en cuenta la ecuación No 6 se genera el valor de riesgo por zona como se evidencia en el Cuadro 29.

Cuadro 29. Valor riesgo por zona

Zonas	Score Criticidad Vulnerabilidades	Cantidad de Activos por Zona	Ponderado Total Criticidad por Zona
1	58	5	11,60
2	32	4	8,00
3	19	3	6,33
4	10	3	3,33

Fuente. Autores

Con el valor ponderado total por zona, se procede a asignar a cada activo dependiendo de la zona en donde pertenece.

Cuadro 30. Activos riesgo por zona

IP	Score 1	Zona	Ponderado Total Criticidad por Zona
192.168.1.11	15	1	11,60
192.168.1.12	18	2	8,00
192.168.1.15	15	2	8,00
192.168.1.15	15	2	8,00
192.168.1.18	18	1	11,60
192.168.1.18	14	1	11,60
192.168.1.2	90	1	11,60
192.168.1.2	72	1	11,60
192.168.1.2	36	1	11,60
192.168.1.5	63	1	11,60
192.168.1.5	35	1	11,60
192.168.1.5	21	1	11,60
192.168.1.7	36	3	6,33
192.168.1.9	10	3	6,33
192.168.2.10	6	4	3,33
192.168.2.13	42	4	3,33
192.168.2.14	90	4	3,33
192.168.2.16	5	3	6,33
192.168.2.16	3	3	6,33
192.168.2.3	18	2	8,00
192.168.2.4	90	2	8,00
192.168.2.4	54	2	8,00
192.168.2.6	18	1	11,60

Fuente. Autores

A continuación se procede aplicar la ecuación No 7 (Score Total) en la cual se realiza la sumatoria del score 1 y el ponderado como se observa en el cuadro 31.

Cuadro 31. Score total

IP	Score 1	Zona	Ponderado Total Criticidad por Zona	Score Total
192.168.1.11	15	1	11,60	26,60
192.168.1.12	18	2	8,00	26,00
192.168.1.15	15	2	8,00	23,00
192.168.1.15	15	2	8,00	23,00
192.168.1.18	18	1	11,60	29,60
192.168.1.18	14	1	11,60	25,60
192.168.1.2	90	1	11,60	101,60
192.168.1.2	72	1	11,60	83,60
192.168.1.2	36	1	11,60	47,60
192.168.1.5	63	1	11,60	74,60
192.168.1.5	35	1	11,60	46,60
192.168.1.5	21	1	11,60	32,60
192.168.1.7	36	3	6,33	42,33
192.168.1.9	10	3	6,33	16,33
192.168.2.10	6	4	3,33	9,33
192.168.2.13	42	4	3,33	45,33
192.168.2.14	90	4	3,33	93,33
192.168.2.16	5	3	6,33	11,33
192.168.2.16	3	3	6,33	9,33
192.168.2.3	18	2	8,00	26,00
192.168.2.4	90	2	8,00	98,00
192.168.2.4	54	2	8,00	62,00
192.168.2.6	18	1	11,60	29,60

Fuente. Autores

Al ordenar del mayor al menor Score Total se obtiene el orden en el cual se deben gestionar las vulnerabilidades, como lo evidencia el Cuadro 32.

Cuadro 32. Orden de gestión de vulnerabilidades

IP	Ambiente	Valoración Activo	Valor Core	Score	Score 1	Zona	Ponderado Total Criticidad por Zona	Score Total
192.168.1.2	Productivo	9	9	81	90	1	11,60	101,60
192.168.2.4	Productivo	9	9	81	90	2	8,00	98,00
192.168.2.14	Productivo	9	9	81	90	4	3,33	93,33
192.168.1.2	Productivo	9	9	63	72	1	11,60	83,60
192.168.1.5	Productivo	7	0	63	63	1	11,60	74,60
192.168.2.4	Productivo	9	9	45	54	2	8,00	62,00
192.168.1.2	Productivo	9	9	27	36	1	11,60	47,60
192.168.1.5	Productivo	7	0	35	35	1	11,60	46,60
192.168.2.13	Productivo	6	0	42	42	4	3,33	45,33
192.168.1.7	Productivo	9	9	27	36	3	6,33	42,33
192.168.1.5	Productivo	7	0	21	21	1	11,60	32,60
192.168.1.18	Desarrollo	2	0	18	18	1	11,60	29,60
192.168.2.6	Desarrollo	2	0	18	18	1	11,60	29,60
192.168.1.11	Productivo	3	0	15	15	1	11,60	26,60
192.168.1.12	Productivo	2	0	18	18	2	8,00	26,00
192.168.2.3	Pruebas	2	0	18	18	2	8,00	26,00
192.168.1.18	Desarrollo	2	0	14	14	1	11,60	25,60
192.168.1.15	Productivo	5	0	15	15	2	8,00	23,00
192.168.1.15	Productivo	5	0	15	15	2	8,00	23,00
192.168.1.9	Desarrollo	2	0	10	10	3	6,33	16,33
192.168.2.16	Pruebas	1	0	5	5	3	6,33	11,33
192.168.2.10	Desarrollo	2	0	6	6	4	3,33	9,33
192.168.2.16	Pruebas	1	0	3	3	3	6,33	9,33

Fuente. Autores

El Cuadro 33 compara cada uno de los cambios en los valores de criticidad dispuesta por la herramienta vs la expuesta en la metodología planteada.

Cuadro 33. Comparación orden de atención

IP	Ambiente	Normativa	Vulnerabilidad	Criticidad	Metodología Actual	Valoración Activo	Valor Core	Score	Score 1	Zona	Ponderado Total Criticidad por Zona	Score Total	Metodología Propuesta
192.168.1.2	Productivo	SOX	P	Critico	1	9	9	81	90	1	11,60	101,60	1
192.168.2.4	Productivo	CSF 042	V	Critico	5	9	9	81	90	2	8,00	98,00	2
192.168.2.14	Productivo	CSF 042	B	Critico	6	9	9	81	90	4	3,33	93,33	3
192.168.1.2	Productivo	SOX	A	Alto	2	9	9	63	72	1	11,60	83,60	4
192.168.1.5	Productivo	PCI	B	Critico	7	7	0	63	63	1	11,60	74,60	5
192.168.2.4	Productivo	CSF 042	H	Medio	13	9	9	45	54	2	8,00	62,00	6
192.168.1.2	Productivo	SOX	S	Bajo	4	9	9	27	36	1	11,60	47,60	7
192.168.1.5	Productivo	PCI	U	Medio	14	7	0	35	35	1	11,60	46,60	8
192.168.2.13	Productivo	SOX	M	Alto	3	6	0	42	42	4	3,33	45,33	9
192.168.1.7	Productivo	CSF 042	T	Bajo	19	9	9	27	36	3	6,33	42,33	10
192.168.1.5	Productivo	PCI	U	Medio	15	7	0	21	21	1	11,60	32,60	11
192.168.1.18	Desarrollo	NA	P	Critico	8	2	0	18	18	1	11,60	29,60	12
192.168.2.6	Desarrollo	NA	I	Critico	9	2	0	18	18	1	11,60	29,60	13
192.168.1.11	Productivo	PCI	L	Medio	16	3	0	15	15	1	11,60	26,60	14
192.168.1.12	Productivo	NA	C	Critico	10	2	0	18	18	2	8,00	26,00	15
192.168.2.3	Pruebas	NA	P	Critico	11	2	0	18	18	2	8,00	26,00	16
192.168.1.18	Desarrollo	NA	D	Alto	12	2	0	14	14	1	11,60	25,60	17
192.168.1.15	Productivo	PCI	E	Bajo	20	5	0	15	15	2	8,00	23,00	18
192.168.1.15	Productivo	PCI	S	Bajo	21	5	0	15	15	2	8,00	23,00	19
192.168.1.9	Desarrollo	NA	L	Medio	17	2	0	10	10	3	6,33	16,33	20
192.168.2.16	Pruebas	NA	U	Medio	18	1	0	5	5	3	6,33	11,33	21
192.168.2.10	Desarrollo	NA	T	Bajo	22	2	0	6	6	4	3,33	9,33	22
192.168.2.16	Pruebas	NA	Q	Bajo	23	1	0	3	3	3	6,33	9,33	23

Fuente. Autores

En el Cuadro 33 se observa que para el activo con dirección IP 192.168.1.2, el escáner de vulnerabilidades (QRadar), determino la vulnerabilidad “A” con una criticidad Alta, la cual con la metodología actual tendría atención en segunda instancia, sin embargo, al aplicar la metodología se observa que debe ser atendida en cuarto lugar, dado que el activo con direcció192.168.2.4, cuya criticidad es crítica debe ser atendida en segundo lugar reduciendo el nivel de exposición, teniendo en cuenta los vectores que son importantes para el Banco de Occidente.

Así mismo se puede observar que el activo con dirección IP 192.168.1.5 la criticidad que ha entregado por el escáner de vulnerabilidades (Qradar) reporto la vulnerabilidad “B” con criticidad de nivel medio en el modelo actual estaría siendo atendida en la posición 14, una vez aplicada la metodología su ponderación 8; esto es producto de la normativa que aplica al activo (PCI), es productivo pese a que no es un activo Core la para el banco, esto no quiere decir que no tenga importancia, pero esta vulnerabilidad podría gestionarse posterior a vulnerabilidades con categorías como la vulnerabilidad “A” del activo 192.168.1.2.

Para los activos con direcciones IP (192.168.1.18, 192.168.2.6, 192.168.2.3 y 192.168.1.11) se observa que la ponderación de las vulnerabilidades permite asignarle otro orden de atención, esto es debido a que estos activos se encuentran en ambientes de desarrollo y pruebas donde no tiene normativa. De esta manera se puede evidenciar que la ponderación de vulnerabilidades mediante el meto propuesto focaliza el esfuerzo en la gestión de vulnerabilidades, brindado prioridad a la gestión, y reduciendo el nivel de exposición.

7. RESULTADOS

7.1 RESULTADOS METODOLOGÍA PROPUESTA

En el Cuadro 34 se relacionan los resultados donde se especifica la cantidad de vulnerabilidades y el tiempo promedio para gestionarlas, teniendo en cuenta el cuadro 8 (criticidad por vulnerabilidad). Para efectos del análisis se excluye las vulnerabilidades de criticidad "Baja" para comparar los dos modelos.

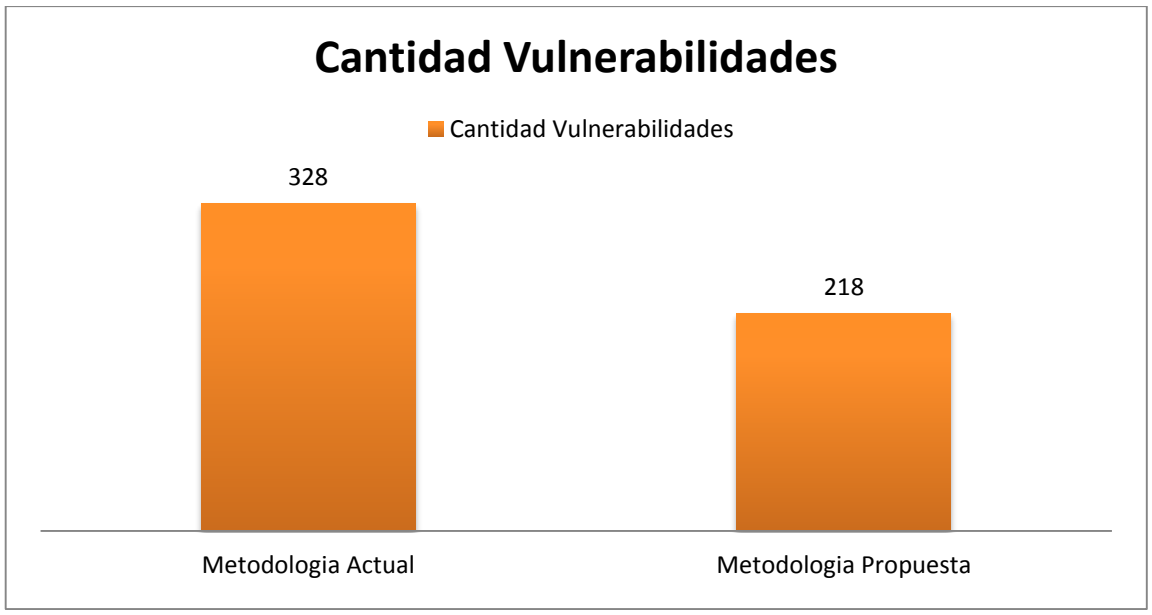
Cuadro 34. Esfuerzo en tiempo para la gestión de vulnerabilidades por criticidad y ambiente en escenario propuesto

Criticidad	Cantidad Vulnerabilidades	Ambiente Productivo + Core	Esfuerzo (min) 1895	Ambiente Productivo No Core	Esfuerzo (min) 748	Ambiente de Pruebas	Esfuerzo (min) 1286	Esfuerzo TOTAL Minutos	Esfuerzo TOTAL HORAS	Esfuerzo TOTAL Días
Criticas	96	18	34110	44	32912	34	43724	110746	1845,8	230,7
Altas	84	10	18950	22	16456	52	66872	102278	1704,6	213,1
Medias	38	6	11370	31	23188	1	1286	35844	597,4	74,7
	218	**34**		**97**		**87**		**248868,0**	**4147,8**	**518,5**

Fuente. Autores

Es destacar que la entidad actualmente excluye las vulnerabilidades de criticidad baja, para realizar la gestión, la cantidad de vulnerabilidades disminuye un 33.5% respecto a la metodología actual como lo ilustra la Gráfica 4.

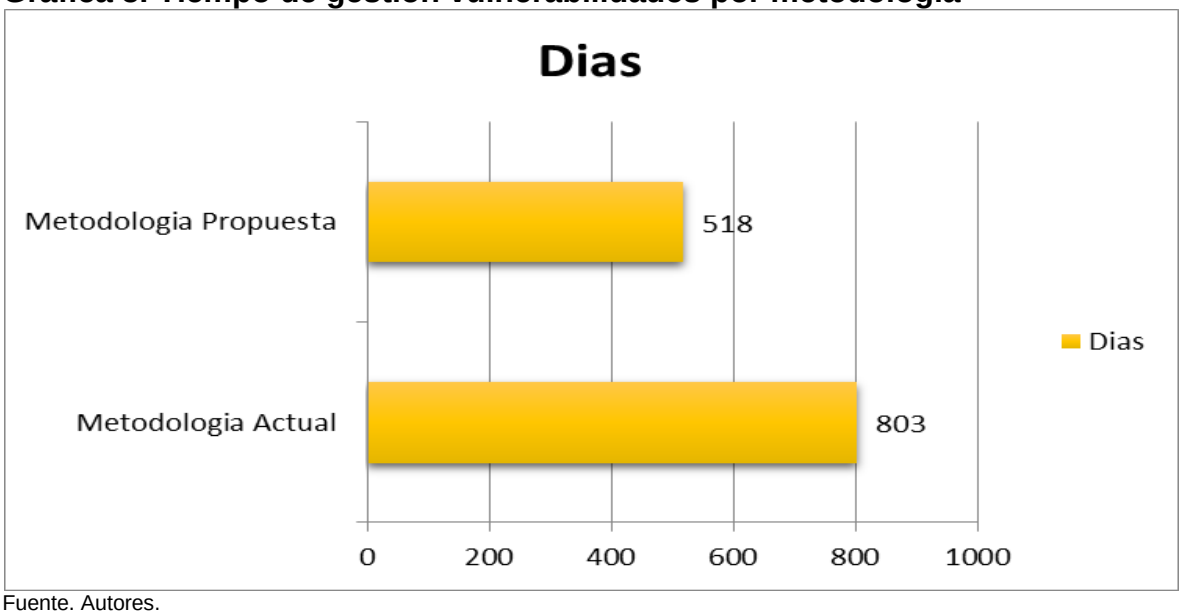
Gráfica 4. Cantidad de vulnerabilidades por metodología



Fuente. Autores.

Teniendo en cuenta el argumento anterior, el tiempo de gestión de las vulnerabilidades disminuye en 35.5% como se ilustra en el Grafico 5.

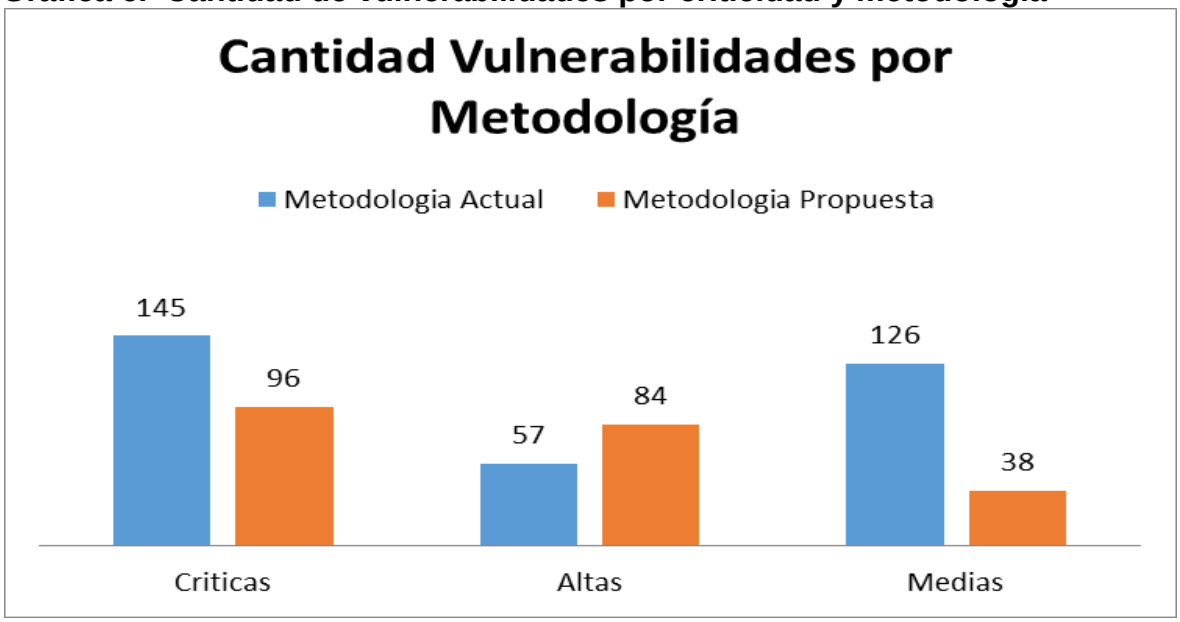
Gráfica 5. Tiempo de gestión vulnerabilidades por metodología



Fuente. Autores.

La metodología propuesta prioriza las vulnerabilidades con mayor nivel de exposición. Para estos datos de prueba, dos de las tres criticidades, su orden de atención varia.

Gráfica 6. Cantidad de vulnerabilidades por criticidad y metodología



Fuente. Autores.

Con la metodología actual se excluyen 54 vulnerabilidades de criticidad baja, a diferencia de la metodología propuesta en la cual 12 de estas, cambiaron su criticidad a media, brindando una mayor visibilidad, determinando un orden de atención.

Cuadro 35. Equipos sin gestionar y con grado medio de exposición

IP	Vulnerabilidad	Criticid	Ambien	Co	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actu	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.89	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Productivo	Si	36	No se gestiona	Medio	203
192.168.29.118	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	Si	36	No se gestiona	Medio	204
192.168.29.61	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	Si	36	No se gestiona	Medio	205
192.168.29.61	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	Si	36	No se gestiona	Medio	206
192.168.29.14	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	Si	28	No se gestiona	Medio	211
192.168.29.101	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	No	27	No se gestiona	Medio	212
192.168.29.101	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Productivo	No	27	No se gestiona	Medio	213
192.168.29.56	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	27	No se gestiona	Medio	214
192.168.29.56	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Productivo	No	27	No se gestiona	Medio	215
192.168.29.16	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	24	No se gestiona	Medio	216
192.168.29.30	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	No	24	No se gestiona	Medio	217
192.168.29.57	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	No	24	No se gestiona	Medio	218

Fuente. Autores

En la metodología actual se identifican vulnerabilidades donde se priorizaron para ser gestionadas, sin embargo, en la metodología propuesta algunas de estas vulnerabilidades presentan una priorización más baja. Esto conlleva a un enfoque desacertado.

Cuadro 36. Nivel de priorización de vulnerabilidades en las dos metodologías

IP	Vulnerabilidad	Criticid	Ambien	Co	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actu	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.47	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Productivo	Si	362	1	Critico	1
192.168.29.47	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	Si	362	1	Critico	2
192.168.29.47	Windows Service Pack Out-of-Date	Critical	Productivo	Si	362	1	Critico	3
192.168.29.14	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Productivo	Si	342	1	Critico	30
192.168.29.89	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Productivo	Si	168	1	Critico	84
192.168.29.89	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Productivo	Si	168	1	Critico	85
192.168.29.118	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	Si	162	1	Critico	86
192.168.29.118	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	Si	162	1	Critico	87
192.168.29.61	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	Productivo	Si	147	1	Critico	89
192.168.29.84	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Productivo	Si	127	1	Critico	94
192.168.29.84	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	Productivo	Si	127	1	Critico	95

Fuente. Autores

En la metodología propuesta 164 vulnerabilidades con criticidad baja no se gestionarían, de las cuales se identificaron 122 vulnerabilidades que si serian gestionadas en la metodología actual. Optimización de recursos.

Cuadro 37. Vulnerabilidades gestionadas en la metodología actual y con criticidad baja en la propuesta

IP	Vulnerabilidad	Criticid	Ambien	Co	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actu	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.72	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	18	7	Bajo	221
192.168.29.72	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	Desarrollo	No	18	7	Bajo	222
192.168.29.78	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	No	18	4	Bajo	223
192.168.29.81	OpenSSL < 0.9.6l Denial of Service	Critical	Desarrollo	No	18	7	Bajo	224
192.168.29.53	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Pruebas	No	18	7	Bajo	225
192.168.29.53	Microsoft SQL Server Unsupported Version Detection	Critical	Pruebas	No	18	7	Bajo	226
192.168.29.53	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Pruebas	No	18	7	Bajo	227
192.168.29.53	Unsupported Unix Operating System	Critical	Pruebas	No	18	7	Bajo	228
192.168.29.60	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	18	7	Bajo	229
192.168.29.60	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Desarrollo	No	18	7	Bajo	230
192.168.29.60	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	Desarrollo	No	18	7	Bajo	231
192.168.29.60	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	Desarrollo	No	18	7	Bajo	232
192.168.29.60	Unsupported Unix Operating System	Critical	Desarrollo	No	18	7	Bajo	233
192.168.29.63	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Pruebas	No	18	7	Bajo	234
192.168.29.64	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Pruebas	No	18	7	Bajo	235
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Pruebas	No	18	7	Bajo	236
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Pruebas	No	18	7	Bajo	237
192.168.29.70	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	Desarrollo	No	18	7	Bajo	238
192.168.29.70	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	Desarrollo	No	18	7	Bajo	239
192.168.29.50	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	14	8	Bajo	240
192.168.29.50	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	14	8	Bajo	241
192.168.29.53	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Pruebas	No	14	8	Bajo	242
192.168.29.60	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Desarrollo	No	14	8	Bajo	243
192.168.29.64	Oracle 9iAS iSQLplus XSS	High	Pruebas	No	14	8	Bajo	244
192.168.29.70	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Desarrollo	No	14	8	Bajo	245
192.168.29.125	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Pruebas	No	10	9	Bajo	246
192.168.29.125	OpenSSL < 0.9.8k Denial of Service	Medium	Pruebas	No	10	9	Bajo	247
192.168.29.18	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	10	9	Bajo	248
192.168.29.18	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Pruebas	No	10	9	Bajo	249
192.168.29.18	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	10	9	Bajo	250
192.168.29.2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Productivo	No	10	6	Bajo	251
192.168.29.2	Web Server Expect Header XSS	Medium	Productivo	No	10	6	Bajo	252
192.168.29.25	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	10	9	Bajo	253
192.168.29.34	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium	Desarrollo	No	10	9	Bajo	254
192.168.29.38	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	10	9	Bajo	255
192.168.29.40	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium	Desarrollo	No	10	9	Bajo	256
192.168.29.71	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	Desarrollo	No	10	9	Bajo	257
192.168.29.71	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Desarrollo	No	10	9	Bajo	258
192.168.29.72	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	Desarrollo	No	10	9	Bajo	259

Cuadro 37 (continuación)

IP	Vulnerabilidad	Criticid	Ambient	Co	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actu	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.46	Web Server Expect Header XSS	Medium	Productivo	No	10	6	Bajo	260
192.168.29.50	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	Desarrollo	No	10	9	Bajo	261
192.168.29.50	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Desarrollo	No	10	9	Bajo	262
192.168.29.53	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Pruebas	No	10	9	Bajo	263
192.168.29.60	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Desarrollo	No	10	9	Bajo	264
192.168.29.60	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	10	9	Bajo	265
192.168.29.60	OpenSSL < 0.9.6f Denial of Service	Medium	Desarrollo	No	10	9	Bajo	266
192.168.29.60	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	Desarrollo	No	10	9	Bajo	267
192.168.29.63	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	10	9	Bajo	268
192.168.29.63	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Pruebas	No	10	9	Bajo	269
192.168.29.63	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Pruebas	No	10	9	Bajo	270
192.168.29.93	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	10	9	Bajo	271
192.168.29.93	OpenSSL < 0.9.8i Denial of Service	Medium	Desarrollo	No	10	9	Bajo	272
192.168.29.94	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Pruebas	No	10	9	Bajo	273
192.168.29.94	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Pruebas	No	10	9	Bajo	274
192.168.29.10	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Desarrollo	No	10	9	Bajo	275
192.168.29.104	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	Desarrollo	No	10	9	Bajo	276
192.168.29.104	OpenSSL < 0.9.6f Denial of Service	Medium	Desarrollo	No	10	9	Bajo	277
192.168.29.104	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Desarrollo	No	10	9	Bajo	278
192.168.29.104	Web Server Expect Header XSS	Medium	Desarrollo	No	10	9	Bajo	279
192.168.29.117	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium	Desarrollo	No	10	9	Bajo	280
192.168.29.117	Symantec AntiVirus Detection (Corporate Edition)	Medium	Desarrollo	No	10	9	Bajo	281
192.168.29.12	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Desarrollo	No	10	9	Bajo	282
192.168.29.12	OpenSSL < 0.9.6k Denial of Service	Medium	Desarrollo	No	10	9	Bajo	283
192.168.29.13	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	Pruebas	No	10	9	Bajo	284
192.168.29.13	Symantec AntiVirus Detection (Corporate Edition)	Medium	Pruebas	No	10	9	Bajo	285
192.168.29.26	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	Desarrollo	No	10	9	Bajo	286
192.168.29.26	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Desarrollo	No	10	9	Bajo	287
192.168.29.26	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	Desarrollo	No	10	9	Bajo	288
192.168.29.41	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Pruebas	No	10	9	Bajo	289
192.168.29.41	OpenSSL < 0.9.8i Denial of Service	Medium	Pruebas	No	10	9	Bajo	290
192.168.29.59	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Productivo	No	10	6	Bajo	291
192.168.29.68	OpenSSL < 0.9.8i Denial of Service	Medium	Desarrollo	No	10	9	Bajo	292
192.168.29.73	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	10	9	Bajo	293
192.168.29.51	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Desarrollo	No	9	7	Bajo	294
192.168.29.51	Oracle Database Unsupported	Critical	Desarrollo	No	9	7	Bajo	295
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Desarrollo	No	9	7	Bajo	296
192.168.29.7	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	9	7	Bajo	297
192.168.29.7	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Pruebas	No	9	7	Bajo	298
192.168.29.7	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Pruebas	No	9	7	Bajo	299
192.168.29.7	Oracle Database Unsupported	Critical	Pruebas	No	9	7	Bajo	300
192.168.29.7	Unsupported Unix Operating System	Critical	Pruebas	No	9	7	Bajo	301
192.168.29.51	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	7	8	Bajo	302
192.168.29.7	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Pruebas	No	7	8	Bajo	303
192.168.29.19	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	5	6	Bajo	325
192.168.29.19	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Productivo	No	5	6	Bajo	326
192.168.29.19	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Productivo	No	5	6	Bajo	327
192.168.29.19	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Productivo	No	5	6	Bajo	328
192.168.29.27	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Desarrollo	No	5	9	Bajo	329
192.168.29.27	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Desarrollo	No	5	9	Bajo	330
192.168.29.27	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	5	9	Bajo	331
192.168.29.27	OpenSSL < 0.9.6k Denial of Service	Medium	Desarrollo	No	5	9	Bajo	332
192.168.29.31	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Desarrollo	No	5	9	Bajo	333
192.168.29.31	OpenSSL < 0.9.6k Denial of Service	Medium	Desarrollo	No	5	9	Bajo	334
192.168.29.31	Web Server Expect Header XSS	Medium	Desarrollo	No	5	9	Bajo	335
192.168.29.35	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Pruebas	No	5	9	Bajo	336
192.168.29.35	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	5	9	Bajo	337
192.168.29.35	OpenSSL < 0.9.6k Denial of Service	Medium	Pruebas	No	5	9	Bajo	338
192.168.29.35	Web Server Expect Header XSS	Medium	Pruebas	No	5	9	Bajo	339
192.168.29.37	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Pruebas	No	5	9	Bajo	340
192.168.29.39	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Desarrollo	No	5	9	Bajo	341
192.168.29.48	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	5	9	Bajo	342
192.168.29.79	OpenSSL < 0.9.6f Denial of Service	Medium	Desarrollo	No	5	9	Bajo	343
192.168.29.80	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	5	9	Bajo	344
192.168.29.80	OpenSSL < 0.9.6k Denial of Service	Medium	Pruebas	No	5	9	Bajo	345
192.168.29.51	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	Desarrollo	No	5	9	Bajo	346
192.168.29.51	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	5	9	Bajo	347
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Desarrollo	No	5	9	Bajo	348
192.168.29.51	Web Server Expect Header XSS	Medium	Desarrollo	No	5	9	Bajo	349
192.168.29.58	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	5	9	Bajo	350
192.168.29.95	OpenSSL < 0.9.8k Denial of Service	Medium	Productivo	No	5	6	Bajo	351
192.168.29.96	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	5	9	Bajo	352
192.168.29.96	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	Pruebas	No	5	9	Bajo	353
192.168.29.96	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	5	9	Bajo	354
192.168.29.97	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	5	9	Bajo	355
192.168.29.97	OpenSSL < 0.9.8l Multiple Vulnerabilities	Medium	Pruebas	No	5	9	Bajo	356
192.168.29.97	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Pruebas	No	5	9	Bajo	357
192.168.29.97	Symantec AntiVirus Detection (Corporate Edition)	Medium	Pruebas	No	5	9	Bajo	358
192.168.29.33	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	5	9	Bajo	359
192.168.29.33	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Pruebas	No	5	9	Bajo	360
192.168.29.7	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	5	9	Bajo	361
192.168.29.7	OpenSSL < 0.9.8i Denial of Service	Medium	Pruebas	No	5	9	Bajo	362
192.168.29.7	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Pruebas	No	5	9	Bajo	363

Fuente. Autores

Vulnerabilidades que cuya clasificación en la metodología actual no están categorizadas como prioritarias, en la metodología actual su nivel de relevancia aumenta. Esto se sustenta porque el valor del “score” es alto, como se aprecia en la Cuadro 38.

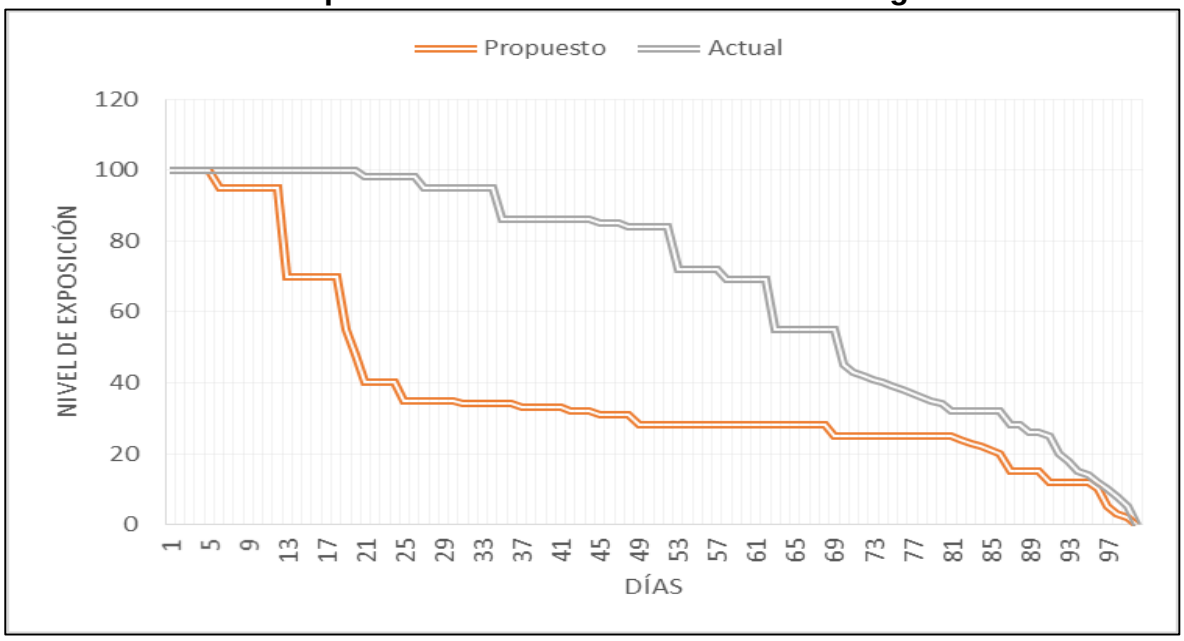
Cuadro 38. Vulnerabilidades críticas en la metodología propuesta y sin priorización en la actual.

IP	Vulnerabilidad	Criticid	Ambien	Co	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actu	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.125	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	286	8	Critico	45
192.168.29.18	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Pruebas	No	286	8	Critico	46
192.168.29.18	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Pruebas	No	286	8	Critico	47
192.168.29.18	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	286	8	Critico	48
192.168.29.25	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Pruebas	No	286	8	Critico	49
192.168.29.38	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Desarrollo	No	286	8	Critico	50
192.168.29.27	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	279	8	Critico	71
192.168.29.35	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	279	8	Critico	72
192.168.29.37	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	279	8	Critico	73
192.168.29.48	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	279	8	Critico	74
192.168.29.93	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	92	8	Alto	104
192.168.29.93	Oracle 9iAS iSQLplus XSS	High	Desarrollo	No	92	8	Alto	105
192.168.29.93	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	92	8	Alto	106
192.168.29.104	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Desarrollo	No	86	8	Alto	125
192.168.29.104	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Desarrollo	No	86	8	Alto	126
192.168.29.104	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Desarrollo	No	86	8	Alto	127
192.168.29.117	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Desarrollo	No	86	8	Alto	128
192.168.29.13	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Pruebas	No	86	8	Alto	129
192.168.29.82	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Pruebas	No	85	8	Alto	130
192.168.29.96	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Pruebas	No	85	8	Alto	131
192.168.29.96	Oracle 9iAS iSQLplus XSS	High	Pruebas	No	85	8	Alto	132
192.168.29.97	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Pruebas	No	85	8	Alto	133
192.168.29.26	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Desarrollo	No	71	8	Alto	154
192.168.29.5	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Pruebas	No	71	8	Alto	155
192.168.29.68	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Desarrollo	No	71	8	Alto	157
192.168.29.68	Oracle 9iAS iSQLplus XSS	High	Desarrollo	No	71	8	Alto	158
192.168.29.33	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	64	8	Alto	161

Fuente. Autores

En la Gráfica 7 se observa el comportamiento del nivel de exposición con la metodología actual y la propuesta, donde se puede determinar la diferencia entre gestionar las vulnerabilidades por grado de exposición (metodología propuesta) y gestionarlas por criticidad y Core (actualmente recursos SOX). Aunque las dos cumplen su objetivo eficazmente, resulta ser más eficiente la metodología propuesta, al disminuir en menor tiempo su nivel de exposición. (En el análisis del grafico se incluyen las vulnerabilidades de criticidad baja).

Gráfica 7. Nivel de exposición con las diferentes metodologías



Fuente. Autores

7.2 SOCIALIZACIÓN DE METODOLOGÍA

Una vez realizado el análisis de los resultados con la información suministrada por el administrador del escáner de vulnerabilidades, se procede a socializar el resultado con el administrador y el Director de Seguridad Informática, quienes ven un aporte de la metodología a la gestión de vulnerabilidades, así mismo brindan aportes como oportunidad de mejora a la metodología la cual consiste en incluir en la clasificación de los activos teniendo en cuenta los accesos con los que cuentan los activos, es decir tener presente los permisos de puertos USB, si dicho activo cuenta con acceso a correo electrónico, si cuenta con acceso internet, con los cuales se puede brindar mayor peso a los activos, ya que son vectores de que pueden utilizar para la explotación de una vulnerabilidad.

Sin embargo esta sugerencia se encuentra fuera del alcance del trabajo, no obstante pueden brindar mejoras a la metodología propuesta, adicionan valor a los activos y a su vez estos asociados a la clasificación de la información incluye mayores pesos a los activos.

Es importante mencionar que la metodología propuesta ha generado interés al Director de Seguridad Informática e informa que este se tendrá como insumo para el proyecto de aseguramiento que se encuentra por iniciar, proyecto que tendría alcance a las entidades del grupo, lo cual para nosotros es de orgullo conocer que la metodología aportara a la estrategia de aseguramiento de la entidad. (Véase Anexo H, I).

8. CONCLUSIONES

- La información de segmentación de redes y la identificación de activos con los diferentes tipos de información, es un insumo fundamental para la re-categorización de vulnerabilidades.

- La re-categorización de vulnerabilidades con la metodología propuesta optimiza los tiempos y recursos a las áreas que realizan la gestión (remediación).

- La metodología propuesta brinda una mayor visibilidad al identificar las vulnerabilidades con mayor nivel de exposición.

- La metodología propuesta, indica ser más eficiente al disminuir en menor tiempo el nivel de exposición.

- La propuesta planteada delimita mejor cuales son las vulnerabilidades con mayor prioridad a gestionar.

9. RECOMENDACIONES

Durante el desarrollo de la metodología se identificaron algunos prerrequisitos importantes que deben cumplirse los cuales se relacionan a continuación:

- Unos de los requisitos calves es la identificación de activos, está es importante tener definida la política de clasificación de la información, así como la respectiva clasificación de activos, dado que para nuestra metodología fue necesario sentarnos con el ingeniero de Seguridad Informática con la finalidad de clasificar los servidores según la aplicación contenida, y tipo de información que maneja.

- Así mismo se debe conocer las diferentes normativas con su respectivo alcance que debe cumplir la Entidad, para las entidades financieras la circular 029 la cual fue actualizada en la circular 029, la detalla los requisitos mínimos que deben cumplir las entidades del sector financiero, así mismo la norma PCI de protección y adecuado manejo de información de tarjetahabientes, otro de las leyes a tener en cuenta es la 1581 ley de protección de datos personales lo cual obliga a las entidades financieras a salvaguardar la información.

- Las herramientas que se utilizan para extraer información para aplicar la metodología son:

    - Escáner de vulnerabilidades QVM, herramienta propietaria de IBM,
    - Firewall,
    - Herramientas de gestión (Ej.: Aranda),
    - Validación de reglas en el firewall para eliminar servicios (puertos) no utilizados.

BIBLIOGRAFÍA

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. ISO/IEC 27001:2005, Tecnología de la Información – Técnicas de seguridad - Sistemas de gestión de Seguridad de la información – Requerimientos [en línea]. Bogotá: La Empresa [Citado el 21 de Noviembre de 2017].Disponible en Internet:

DEFINICIÓN ABC. Definición Infraestructura. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.definicionabc.com

FIRST. Common Vulnerability Scoring System v3.0. Calculator. 1998. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <. https://www.first.org/cvss/calculator/3.0

INFOSPY WARE. Definición Malware. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.infospyware.com

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN – ICONTEC. NTC 1486 Documentación. Presentación de tesis, trabajos de grado y otros documentos de investigación. Sexta Actualización. NTC5613 Referencias bibliográficas. Contenido y estructura. NTC 4490. Referencias documentales para fuentes de información electrónicas. Bogotá D.C.: ICONTEC. 2018, 92p.

JIMÉNEZ, Milenys. Seguridad e Higiene Industrial SHI. Universidad Nacional Abierta. Centro LOCAL Cojedes, Citado el 21 de Noviembre de 2017). Disponible en Internet: < shi-unacojedes.wikispaces.com/Nivel+de+Exposición

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE COLOMBIA. Guía para la gestión y clasificación de activos de información – MinTic. . (Citado el 21 de Noviembre de 2017). Disponible en Internet: < (https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE COLOMBIA. Modelo nacional de gestión de riesgos de seguridad digital. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <www.mintic.gov.co/portal/604/articles-61854_documento.docx.

REAL ACADEMIA ESPAÑOLA-RAE. (2014). Tarjetahabiente. (33 ed.). Madrid: ASALE.

SECURITY STADARDS COUNCIL. Definición de vulnerabilidad. Citado el 21 de Noviembre de 2017). Disponible en Internet: < (https://es.pcisecuritystandards.org.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 029/14 Bogotá D.C. Superfinanciera. 2014. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <https://www.superfinanciera.gov.co/publicacion/circular-basica-juridica-c-e-029-14-10083443

TILVES, Mónica. Cada 3.75 segundos surge un nuevo malware Windows. Silicon. 2015. (Citado el 21 de Noviembre de 2017). Disponible en Internet: <. http://www.silicon.es/cada-375-segundos-surge-un-nuevo-malware-para-windows-82057

WELIVESECURITY. Análisis de vulnerabilidad. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < www.welivesecurity.com.

WELIVESECURITY. Vulnerabilidades-que-es-cvss-como-utilizarlo. (Citado el 21 de Noviembre de 2017). Disponible en Internet: < https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

ANEXOS

ANEXO A

CONSOLIDADO ENTREVISTA ADMINISTRADORES TI

	Valida usted que la vulnerabilidad aplique a la plataforma que Usted administra?	Cual es el tiempo (minutos) invertido en la validacion que una vulenrabilidad corresponde al sitema adminitrado?	Usted realiza documentación sobre el problema que ocasiona la vulnerabilidad?	Tiempo (minutos) que invierte para realizar la documentación?	Una vez entregado el reporte, generar un plan de acción para implementar la remediacion de la vulnerabilidad?	Especifique el tiempo (minutos) que invierte para realizar el plan de acción (paso a paso)
Soporte Windows	si	30 minutos	si	180 minutos	No	90 minutos
Bases de Datos	si	10 minutos	No	0	si	10 minutos por vulnerabilidad
AIX/Linux	si	5 minutos	si	30 minutos	si	60 minutos
Aplicación	si	15 minutos	si	30 minutos	si	120 minutos
Web	Si	15 minutos	si	30 minutos	si	30 minutos
Soporte Usuarios	Si, y solo se gestionan las vulnerabilidades altas por el volumen tan alto de equipos	30 minutos	No	0	si	30 minutos
Telecomunicaciones	SI	15 minutos	No	0	si	45 minutos
Promedio		17,15		67,5		59,28

Usted generar un control de cambios, para la aplicación de las vulnerabilidades?	Que tiempo (minutos) es requerido para la autorización y aplicación de la remediación de la vulnerabilidad de un ambiente Core	Para aplicar la remediación de una vulnerabilidad, ya sea una actualización o un parche, la aplica previamente en ambiente de pruebas?	Indique el tiempo (minutos) requerido para la aplicación de la vulnerabilidad, en ambiente pruebas?	Tiempo (minutos) requerido para validar, que la aplicación de la vulnerabilidad no afectan la funcionalidad del activo de información para el objetivo de negocio.	Indique el tiempo que invierte para aplicar la actualización en ambiente productivo?	Tiempo (minutos) que invierte para validar, si no generan ningún tipo de indisponibilidad en el negocio, la aplicación de la vulnerabilidad que tiempo requiere
Si	cambios de emergencia 24 horas, si no es de emergencia 15 días	No	24 horas emergencia, 15 días programo	1440 minutos	Coordinar con administradores, ventana de tiempo, pruebas, 24 horas	240 minutos
Si	Depende de la disponibilidad del ambiente en promedio de 1 a 2 semanas	si	Esto depende del tipo de remediación debido a que hay que generar backups de las plataformas antes de aplicar la remediación , pero en promedio seria de 1 a 2 horas con validaciones	4800 minutos	Esto depende del tipo de remediación debido a que hay que generar backups de las plataformas antes de aplicar la remediación , pero en promedio seria de 1 a 2 horas con validaciones	30 minutos
Si	30 minutos	Desarrollo, posteriormente en pruebas	30 minutos	30 minutos	30 minutos	30 minutos
Si	120 minutos	si	120 minutos	30 minutos	120 minutos	30 minutos
Si	30 minutos	si	30 minutos	30 minutos	60 minutos	30 minutos
No	No	si	15 minutos	960 minutos	240	2800 minutos
Si	30 minutos	no, no hay un ambiente de pruebas	5 minutos	10 minutos	60 minutos	10 minutos
	52,5		58,33	1042	102	452

ANEXO B.

ACTIVOS DE INFORMACIÓN POR AMBIENTE Y CORE

IP	Ambiente	Core	IP	Ambiente	Core	IP	Ambiente	Core
192.168.29.10	Desarrollo	No	192.168.29.35	Pruebas	No	192.168.29.68	Desarrollo	No
192.168.29.101	Productivo	No	192.168.29.37	Pruebas	No	192.168.29.69	Productivo	No
192.168.29.104	Desarrollo	No	192.168.29.38	Desarrollo	No	192.168.29.7	Pruebas	No
192.168.29.117	Desarrollo	No	192.168.29.39	Desarrollo	No	192.168.29.70	Desarrollo	No
192.168.29.118	Productivo	Si	192.168.29.40	Desarrollo	No	192.168.29.71	Desarrollo	No
192.168.29.12	Desarrollo	No	192.168.29.41	Pruebas	No	192.168.29.72	Desarrollo	No
192.168.29.120	Productivo	No	192.168.29.43	Productivo	No	192.168.29.73	Pruebas	No
192.168.29.125	Pruebas	No	192.168.29.46	Productivo	No	192.168.29.76	Productivo	No
192.168.29.13	Pruebas	No	192.168.29.47	Productivo	Si	192.168.29.77	Productivo	No
192.168.29.14	Productivo	Si	192.168.29.48	Pruebas	No	192.168.29.78	Productivo	No
192.168.29.16	Productivo	No	192.168.29.49	Productivo	No	192.168.29.79	Desarrollo	No
192.168.29.18	Pruebas	No	192.168.29.5	Pruebas	No	192.168.29.80	Pruebas	No
192.168.29.19	Productivo	No	192.168.29.50	Desarrollo	No	192.168.29.81	Desarrollo	No
192.168.29.2	Productivo	No	192.168.29.51	Desarrollo	No	192.168.29.82	Pruebas	No
192.168.29.21	Productivo	No	192.168.29.53	Pruebas	No	192.168.29.84	Productivo	Si
192.168.29.23	Productivo	No	192.168.29.55	Productivo	No	192.168.29.88	Productivo	No
192.168.29.24	Productivo	Si	192.168.29.56	Productivo	No	192.168.29.89	Productivo	Si
192.168.29.25	Pruebas	No	192.168.29.57	Productivo	No	192.168.29.93	Desarrollo	No
192.168.29.26	Desarrollo	No	192.168.29.58	Pruebas	No	192.168.29.94	Pruebas	No
192.168.29.27	Desarrollo	No	192.168.29.59	Productivo	No	192.168.29.95	Productivo	No
192.168.29.30	Productivo	No	192.168.29.60	Desarrollo	No	192.168.29.96	Pruebas	No
192.168.29.31	Desarrollo	No	192.168.29.61	Productivo	Si	192.168.29.97	Pruebas	No
192.168.29.33	Pruebas	No	192.168.29.63	Pruebas	No			
192.168.29.34	Desarrollo	No	192.168.29.64	Pruebas	No			

ANEXO C.
TOTAL DE VULNERABILIDADES

IP	Vulnerabilidad	Criticidad
192.168.29.10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.10	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium
192.168.29.10	Unsupported Unix Operating System	Critical
192.168.29.101	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low
192.168.29.101	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.101	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
192.168.29.101	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical
192.168.29.101	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.101	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium
192.168.29.101	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.101	OpenSSL < 0.9.8 Weak Default Configuration	Medium
192.168.29.101	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High
192.168.29.101	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.101	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium
192.168.29.101	Windows Service Pack Out-of-Date	Critical
192.168.29.104	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.104	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.104	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium
192.168.29.104	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical
192.168.29.104	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.104	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.104	OpenSSL < 0.9.8 Weak Default Configuration	Medium
192.168.29.104	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High
192.168.29.104	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.104	Web Server Expect Header XSS	Medium
192.168.29.104	Windows Service Pack Out-of-Date	Critical
192.168.29.117	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.117	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium
192.168.29.117	Symantec AntiVirus Detection (Corporate Edition)	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.118	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low
192.168.29.118	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.118	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical
192.168.29.118	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium
192.168.29.118	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium
192.168.29.118	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium
192.168.29.118	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.118	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.12	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.12	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.12	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.12	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.12	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.12	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.120	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.120	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical
192.168.29.120	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.120	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.120	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.120	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.120	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.120	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.120	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.120	OpenSSL < 0.9.8j Signature Spoofing	Critical
192.168.29.120	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium
192.168.29.120	Windows Service Pack Out-of-Date	Critical
192.168.29.125	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium
192.168.29.125	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.125	OpenSSL < 0.9.8k Denial of Service	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.125	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.13	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium
192.168.29.13	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	Critical
192.168.29.13	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.13	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
192.168.29.13	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.13	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.13	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical
192.168.29.13	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical
192.168.29.13	Symantec AntiVirus Detection (Corporate Edition)	Medium
192.168.29.13	Unsupported Unix Operating System	Critical
192.168.29.14	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.14	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.14	OpenSSL < 0.9.8 Weak Default Configuration	Medium
192.168.29.16	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.16	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.16	Symantec AntiVirus Detection (Corporate Edition)	Medium
192.168.29.18	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.18	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium
192.168.29.18	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical
192.168.29.18	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.18	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.18	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.18	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.18	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.18	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.19	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical
192.168.29.19	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.19	Microsoft SQL Server Unsupported Version Detection	Critical

IP	Vulnerabilidad	Criticidad
192.168.29.19	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.19	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
192.168.29.19	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.19	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.19	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.19	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.19	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical
192.168.29.19	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.19	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.2	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.2	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium
192.168.29.2	Web Server Expect Header XSS	Medium
192.168.29.21	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.21	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical
192.168.29.21	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.21	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.23	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium
192.168.29.23	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.23	OpenSSL < 0.9.8k Denial of Service	Medium
192.168.29.23	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical
192.168.29.24	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium
192.168.29.24	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.24	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.24	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.25	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.25	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.25	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.25	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High

IP	Vulnerabilidad	Criticidad
192.168.29.26	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.26	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium
192.168.29.26	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical
192.168.29.26	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.26	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical
192.168.29.26	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.26	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High
192.168.29.26	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.26	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium
192.168.29.26	Oracle Database Unsupported	Critical
192.168.29.26	Windows Service Pack Out-of-Date	Critical
192.168.29.27	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical
192.168.29.27	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.27	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.27	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.27	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.27	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.27	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.27	Windows Service Pack Out-of-Date	Critical
192.168.29.30	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.30	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.30	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.31	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium
192.168.29.31	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.31	Web Server Expect Header XSS	Medium
192.168.29.33	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.33	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.33	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.33	OpenSSL < 0.9.6l Denial of Service	Critical

IP	Vulnerabilidad	Criticidad
192.168.29.33	OpenSSL < 0.9.8j Signature Spoofing	Critical
192.168.29.33	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium
192.168.29.34	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical
192.168.29.34	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.34	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium
192.168.29.35	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical
192.168.29.35	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.35	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical
192.168.29.35	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium
192.168.29.35	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.35	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.35	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.35	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.35	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.35	Web Server Expect Header XSS	Medium
192.168.29.37	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.37	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.37	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	Critical
192.168.29.37	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical
192.168.29.37	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.37	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.37	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.38	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.38	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.38	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.39	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.39	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.39	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.40	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.40	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.40	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.41	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.41	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium
192.168.29.41	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.43	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.43	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical
192.168.29.43	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
192.168.29.43	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical
192.168.29.43	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.43	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.43	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.43	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical
192.168.29.43	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.46	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical
192.168.29.46	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical
192.168.29.46	Unsupported Unix Operating System	Critical
192.168.29.46	Web Server Expect Header XSS	Medium
192.168.29.47	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.47	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.47	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical
192.168.29.47	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.47	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.47	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.47	Oracle 9iAS iSQLplus XSS	High
192.168.29.47	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.47	Web Server Expect Header XSS	Medium
192.168.29.47	Windows Service Pack Out-of-Date	Critical
192.168.29.48	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High

IP	Vulnerabilidad	Criticidad
192.168.29.48	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.48	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.48	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.48	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.48	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical
192.168.29.48	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical
192.168.29.48	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.48	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.49	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.49	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.49	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.49	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.49	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical
192.168.29.49	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.5	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.5	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.5	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.50	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium
192.168.29.50	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.50	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.50	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.51	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.51	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium
192.168.29.51	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical
192.168.29.51	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.51	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.51	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.51	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.51	Oracle Database Unsupported	Critical

IP	Vulnerabilidad	Criticidad
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium
192.168.29.51	Web Server Expect Header XSS	Medium
192.168.29.53	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.53	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.53	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.53	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium
192.168.29.53	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.53	Unsupported Unix Operating System	Critical
192.168.29.55	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.55	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.56	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.56	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.56	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.56	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High
192.168.29.56	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.56	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical
192.168.29.56	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium
192.168.29.57	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.57	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical
192.168.29.57	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.57	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium
192.168.29.57	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.57	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.57	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.57	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.57	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium
192.168.29.57	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.58	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical

IP	Vulnerabilidad	Criticidad
192.168.29.58	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.58	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.58	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.59	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical
192.168.29.59	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical
192.168.29.59	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical
192.168.29.59	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low
192.168.29.59	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.59	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.59	OpenSSL < 0.9.8 Weak Default Configuration	Medium
192.168.29.59	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.59	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.59	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.59	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical
192.168.29.60	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.60	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.60	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.60	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical
192.168.29.60	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.60	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical
192.168.29.60	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.60	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium
192.168.29.60	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical
192.168.29.60	Unsupported Unix Operating System	Critical
192.168.29.61	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low
192.168.29.61	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low
192.168.29.61	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical
192.168.29.63	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.63	OpenSSL < 0.9.8 Weak Default Configuration	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.63	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium
192.168.29.63	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical
192.168.29.64	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.64	Oracle 9iAS iSQLplus XSS	High
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical
192.168.29.68	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.68	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.68	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.68	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical
192.168.29.68	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.68	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.68	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.68	Oracle 9iAS iSQLplus XSS	High
192.168.29.68	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical
192.168.29.69	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High
192.168.29.69	Microsoft SQL Server Unsupported Version Detection	Critical
192.168.29.7	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.7	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.7	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.7	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.7	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical
192.168.29.7	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.7	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High
192.168.29.7	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.7	Oracle Database Unsupported	Critical
192.168.29.7	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium
192.168.29.7	Unsupported Unix Operating System	Critical
192.168.29.70	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical

IP	Vulnerabilidad	Criticidad
192.168.29.70	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical
192.168.29.70	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.70	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.71	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.71	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.71	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium
192.168.29.71	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium
192.168.29.72	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.72	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium
192.168.29.72	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low
192.168.29.72	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical
192.168.29.73	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical
192.168.29.73	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium
192.168.29.73	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.76	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.76	Oracle 9iAS iSQLplus XSS	High
192.168.29.77	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.78	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical
192.168.29.79	OpenSSL < 0.9.6f Denial of Service	Medium
192.168.29.80	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium
192.168.29.80	OpenSSL < 0.9.6k Denial of Service	Medium
192.168.29.81	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low
192.168.29.81	OpenSSL < 0.9.6l Denial of Service	Critical
192.168.29.82	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.82	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.84	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical
192.168.29.84	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical
192.168.29.88	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical
192.168.29.88	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.88	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.88	OpenSSL < 0.9.8 Weak Default Configuration	Medium
192.168.29.88	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.88	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical
192.168.29.89	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High
192.168.29.89	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.89	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical
192.168.29.89	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical
192.168.29.93	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.93	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium
192.168.29.93	OpenSSL < 0.9.8i Denial of Service	Medium
192.168.29.93	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.93	Oracle 9iAS iSQLplus XSS	High
192.168.29.93	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High
192.168.29.94	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical
192.168.29.94	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical
192.168.29.94	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium
192.168.29.94	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium
192.168.29.94	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low
192.168.29.94	OpenSSL < 0.9.8j Signature Spoofing	Critical
192.168.29.95	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical
192.168.29.95	OpenSSL < 0.9.8k Denial of Service	Medium
192.168.29.96	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low
192.168.29.96	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.96	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium
192.168.29.96	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium
192.168.29.96	OpenSSL < 0.9.8u Multiple Vulnerabilities	High
192.168.29.96	Oracle 9iAS iSQLplus XSS	High
192.168.29.97	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium
192.168.29.97	OpenSSL < 0.9.8l Multiple Vulnerabilities	Medium

IP	Vulnerabilidad	Criticidad
192.168.29.97	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low
192.168.29.97	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High
192.168.29.97	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium
192.168.29.97	Symantec AntiVirus Detection (Corporate Edition)	Medium

ANEXO D
RESPUESTA SEGURIDAD INFORMÁTICA

Responder | Eliminar Correo no deseado | •••

RE: Confirmacion de orden de remediacion de vulnerabilidades actual

Daniel Infante Godoy< DInfante@bancodeoccidente.com.co>
Hoy 11:52 a.m.
David Fernando Ramirez Leon (DRamirezL@bancodeoccidente.com.co)

Responder

Hola David buenos días,

El escáner con el que contamos emite calificaciones de riesgo (Alto, Medio, Bajo y Alerta), la atención de las vulnerabilidades la tenemos concentrada por estrategia en atención primero a plataforma SOX y luego a plataforma No-SOX iniciando con Altas y luego Medias, para cada grupo de especialistas; en la práctica, sin embargo, hay muchas que primero se atienden en plataforma No-Sox debido al procedimiento de control de cambios en donde debemos primero realizar pruebas, validar calidad, impacto y tiempo de estabilización, antes de poder implementar los cambios en producción.

Recogiendo la forma como lo colocas, el orden por estrategia es el siguiente, con las consideraciones mencionadas:

Atención 1

- Vulnerabilidades Altas ambiente productivo core SOX
- Vulnerabilidades Medias ambiente productivo core SOX

Atención 2

- Vulnerabilidades Altas ambiente productivo core no SOX
- Vulnerabilidades Medias ambiente productivo core no SOX

Banco de Occidente

Daniel Infante Godoy
Ingeniero de Seguridad Informática | Gerencia de Tecnología
Vicepresidencia de Operaciones y Tecnología

Tel: (1) 756 0999 - 17789 - DG Bogotá
Email: Dinfante@bancodeoccidente.com.co
www.bancodeoccidente.com.co

ANEXO E

DATOS METODOLOGÍA ACTUAL

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.47	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Productivo	Si	1
192.168.29.47	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	Si	1
192.168.29.47	Windows Service Pack Out-of-Date	Critical	Productivo	Si	1
192.168.29.14	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Productivo	Si	1
192.168.29.89	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Productivo	Si	1
192.168.29.89	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Productivo	Si	1
192.168.29.118	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	Si	1
192.168.29.118	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	Si	1
192.168.29.61	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	Productivo	Si	1
192.168.29.84	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Productivo	Si	1
192.168.29.84	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	Productivo	Si	1
192.168.29.24	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Productivo	Si	2
192.168.29.47	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Productivo	Si	2
192.168.29.47	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Productivo	Si	2
192.168.29.47	Oracle 9iAS iSQLplus XSS	High	Productivo	Si	2
192.168.29.47	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Productivo	Si	2
192.168.29.89	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Productivo	Si	2
192.168.29.118	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Productivo	Si	2
192.168.29.24	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Productivo	Si	3
192.168.29.24	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Productivo	Si	3
192.168.29.24	OpenSSL < 0.9.8i Denial of Service	Medium	Productivo	Si	3
192.168.29.47	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Productivo	Si	3
192.168.29.47	OpenSSL < 0.9.8i Denial of Service	Medium	Productivo	Si	3
192.168.29.47	Web Server Expect Header XSS	Medium	Productivo	Si	3
192.168.29.118	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	Productivo	Si	3
192.168.29.118	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Productivo	Si	3
192.168.29.118	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	Productivo	Si	3
192.168.29.118	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Productivo	Si	3
192.168.29.14	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Productivo	Si	3

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.101	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Productivo	No	4
192.168.29.101	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	Productivo	No	4
192.168.29.101	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Productivo	No	4
192.168.29.101	Windows Service Pack Out-of-Date	Critical	Productivo	No	4
192.168.29.43	Microsoft SQL Server Unsupported Version Detection	Critical	Productivo	No	4
192.168.29.43	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	Productivo	No	4
192.168.29.43	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Productivo	No	4
192.168.29.43	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	Productivo	No	4
192.168.29.43	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Productivo	No	4
192.168.29.43	OpenSSL < 0.9.6l Denial of Service	Critical	Productivo	No	4
192.168.29.43	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Productivo	No	4
192.168.29.120	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	Productivo	No	4
192.168.29.120	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	No	4
192.168.29.120	OpenSSL < 0.9.6l Denial of Service	Critical	Productivo	No	4
192.168.29.120	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.120	OpenSSL < 0.9.8j Signature Spoofing	Critical	Productivo	No	4
192.168.29.120	Windows Service Pack Out-of-Date	Critical	Productivo	No	4
192.168.29.16	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Productivo	No	4
192.168.29.21	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	Productivo	No	4
192.168.29.23	OpenSSL < 0.9.6l Denial of Service	Critical	Productivo	No	4
192.168.29.23	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Productivo	No	4
192.168.29.19	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.19	Microsoft SQL Server Unsupported Version Detection	Critical	Productivo	No	4
192.168.29.19	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Productivo	No	4
192.168.29.19	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Productivo	No	4
192.168.29.56	Microsoft SQL Server Unsupported Version Detection	Critical	Productivo	No	4
192.168.29.56	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Productivo	No	4
192.168.29.57	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	Productivo	No	4
192.168.29.57	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Productivo	No	4

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.57	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.55	Microsoft SQL Server Unsupported Version Detection	Critical	Productivo	No	4
192.168.29.88	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	No	4
192.168.29.88	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Productivo	No	4
192.168.29.69	Microsoft SQL Server Unsupported Version Detection	Critical	Productivo	No	4
192.168.29.46	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.46	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Productivo	No	4
192.168.29.46	Unsupported Unix Operating System	Critical	Productivo	No	4
192.168.29.95	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Productivo	No	4
192.168.29.59	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.59	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	No	4
192.168.29.59	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical	Productivo	No	4
192.168.29.59	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Productivo	No	4
192.168.29.59	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Productivo	No	4
192.168.29.59	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	Productivo	No	4
192.168.29.49	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Productivo	No	4
192.168.29.49	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Productivo	No	4
192.168.29.49	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Productivo	No	4
192.168.29.78	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	Productivo	No	4
192.168.29.101	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Productivo	No	5
192.168.29.101	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Productivo	No	5
192.168.29.43	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Productivo	No	5
192.168.29.43	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Productivo	No	5
192.168.29.21	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Productivo	No	5
192.168.29.19	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Productivo	No	5
192.168.29.56	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Productivo	No	5
192.168.29.57	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Productivo	No	5
192.168.29.57	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Productivo	No	5
192.168.29.69	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Productivo	No	5

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.76	Oracle 9iAS iSQLplus XSS	High	Productivo	No	5
192.168.29.77	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Productivo	No	5
192.168.29.59	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Productivo	No	5
192.168.29.49	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Productivo	No	5
192.168.29.49	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Productivo	No	5
192.168.29.101	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Productivo	No	6
192.168.29.101	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Productivo	No	6
192.168.29.101	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Productivo	No	6
192.168.29.101	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	Productivo	No	6
192.168.29.56	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	6
192.168.29.56	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Productivo	No	6
192.168.29.120	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	6
192.168.29.120	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Productivo	No	6
192.168.29.120	OpenSSL < 0.9.6f Denial of Service	Medium	Productivo	No	6
192.168.29.120	OpenSSL < 0.9.6k Denial of Service	Medium	Productivo	No	6
192.168.29.120	OpenSSL < 0.9.8i Denial of Service	Medium	Productivo	No	6
192.168.29.120	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium	Productivo	No	6
192.168.29.16	Symantec AntiVirus Detection (Corporate Edition)	Medium	Productivo	No	6
192.168.29.21	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Productivo	No	6
192.168.29.21	OpenSSL < 0.9.6f Denial of Service	Medium	Productivo	No	6
192.168.29.23	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	Productivo	No	6
192.168.29.23	OpenSSL < 0.9.8k Denial of Service	Medium	Productivo	No	6
192.168.29.30	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	6
192.168.29.30	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Productivo	No	6
192.168.29.57	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	Productivo	No	6
192.168.29.57	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Productivo	No	6
192.168.29.57	OpenSSL < 0.9.6f Denial of Service	Medium	Productivo	No	6
192.168.29.57	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium	Productivo	No	6
192.168.29.76	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Productivo	No	6

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.88	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Productivo	No	6
192.168.29.88	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Productivo	No	6
192.168.29.88	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Productivo	No	6
192.168.29.49	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	6
192.168.29.2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Productivo	No	6
192.168.29.2	Web Server Expect Header XSS	Medium	Productivo	No	6
192.168.29.46	Web Server Expect Header XSS	Medium	Productivo	No	6
192.168.29.59	OpenSSL < 0.9.8 Weak Default Configuration	Medium	Productivo	No	6
192.168.29.19	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Productivo	No	6
192.168.29.19	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Productivo	No	6
192.168.29.19	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Productivo	No	6
192.168.29.19	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Productivo	No	6
192.168.29.95	OpenSSL < 0.9.8k Denial of Service	Medium	Productivo	No	6
192.168.29.125	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Pruebas	No	7
192.168.29.18	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	Pruebas	No	7
192.168.29.18	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Pruebas	No	7
192.168.29.18	OpenSSL < 0.9.6l Denial of Service	Critical	Pruebas	No	7
192.168.29.25	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	7
192.168.29.34	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical	Desarrollo	No	7
192.168.29.34	OpenSSL < 0.9.6l Denial of Service	Critical	Desarrollo	No	7
192.168.29.38	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Desarrollo	No	7
192.168.29.40	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Desarrollo	No	7
192.168.29.27	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	Desarrollo	No	7
192.168.29.27	Windows Service Pack Out-of-Date	Critical	Desarrollo	No	7
192.168.29.35	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	Pruebas	No	7
192.168.29.35	Microsoft SQL Server Unsupported Version Detection	Critical	Pruebas	No	7
192.168.29.35	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	Pruebas	No	7
192.168.29.35	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Pruebas	No	7
192.168.29.37	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Pruebas	No	7

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.37	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	Critical	Pruebas	No	7
192.168.29.37	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	Pruebas	No	7
192.168.29.37	OpenSSL < 0.9.6l Denial of Service	Critical	Pruebas	No	7
192.168.29.48	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	7
192.168.29.48	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	Pruebas	No	7
192.168.29.48	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical	Pruebas	No	7
192.168.29.48	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Pruebas	No	7
192.168.29.48	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Pruebas	No	7
192.168.29.93	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Desarrollo	No	7
192.168.29.94	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	Pruebas	No	7
192.168.29.94	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	Pruebas	No	7
192.168.29.94	OpenSSL < 0.9.8j Signature Spoofing	Critical	Pruebas	No	7
192.168.29.10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.10	Unsupported Unix Operating System	Critical	Desarrollo	No	7
192.168.29.104	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.104	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	Desarrollo	No	7
192.168.29.104	OpenSSL < 0.9.6l Denial of Service	Critical	Desarrollo	No	7
192.168.29.104	Windows Service Pack Out-of-Date	Critical	Desarrollo	No	7
192.168.29.12	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.12	OpenSSL < 0.9.6l Denial of Service	Critical	Desarrollo	No	7
192.168.29.13	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	Critical	Pruebas	No	7
192.168.29.13	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	Pruebas	No	7
192.168.29.13	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	Pruebas	No	7
192.168.29.13	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical	Pruebas	No	7
192.168.29.13	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	Pruebas	No	7
192.168.29.13	Unsupported Unix Operating System	Critical	Pruebas	No	7
192.168.29.58	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	Pruebas	No	7
192.168.29.58	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Pruebas	No	7
192.168.29.82	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Pruebas	No	7

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.26	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.26	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical	Desarrollo	No	7
192.168.29.26	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Desarrollo	No	7
192.168.29.26	Oracle Database Unsupported	Critical	Desarrollo	No	7
192.168.29.26	Windows Service Pack Out-of-Date	Critical	Desarrollo	No	7
192.168.29.5	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	7
192.168.29.5	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Pruebas	No	7
192.168.29.68	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.68	Microsoft SQL Server Unsupported Version Detection	Critical	Desarrollo	No	7
192.168.29.68	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	Desarrollo	No	7
192.168.29.68	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	Desarrollo	No	7
192.168.29.68	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Desarrollo	No	7
192.168.29.33	OpenSSL < 0.9.6l Denial of Service	Critical	Pruebas	No	7
192.168.29.33	OpenSSL < 0.9.8j Signature Spoofing	Critical	Pruebas	No	7
192.168.29.73	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	7
192.168.29.72	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.72	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.81	OpenSSL < 0.9.6l Denial of Service	Critical	Desarrollo	No	7
192.168.29.53	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Pruebas	No	7
192.168.29.53	Microsoft SQL Server Unsupported Version Detection	Critical	Pruebas	No	7
192.168.29.53	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Pruebas	No	7
192.168.29.53	Unsupported Unix Operating System	Critical	Pruebas	No	7
192.168.29.60	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	Desarrollo	No	7
192.168.29.60	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Desarrollo	No	7
192.168.29.60	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	Desarrollo	No	7
192.168.29.60	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	Desarrollo	No	7
192.168.29.60	Unsupported Unix Operating System	Critical	Desarrollo	No	7
192.168.29.63	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Pruebas	No	7
192.168.29.64	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	Pruebas	No	7

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	Pruebas	No	7
192.168.29.64	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Pruebas	No	7
192.168.29.70	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	Desarrollo	No	7
192.168.29.70	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	Desarrollo	No	7
192.168.29.51	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Desarrollo	No	7
192.168.29.51	Oracle Database Unsupported	Critical	Desarrollo	No	7
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	Desarrollo	No	7
192.168.29.7	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	Pruebas	No	7
192.168.29.7	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	Pruebas	No	7
192.168.29.7	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	Pruebas	No	7
192.168.29.7	Oracle Database Unsupported	Critical	Pruebas	No	7
192.168.29.7	Unsupported Unix Operating System	Critical	Pruebas	No	7
192.168.29.125	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	8
192.168.29.18	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Pruebas	No	8
192.168.29.18	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Pruebas	No	8
192.168.29.18	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	8
192.168.29.25	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Pruebas	No	8
192.168.29.38	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Desarrollo	No	8
192.168.29.27	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	8
192.168.29.35	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Pruebas	No	8
192.168.29.37	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	8
192.168.29.48	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	8
192.168.29.93	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	8
192.168.29.93	Oracle 9iAS iSQLplus XSS	High	Desarrollo	No	8
192.168.29.93	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	8
192.168.29.104	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Desarrollo	No	8
192.168.29.104	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Desarrollo	No	8
192.168.29.104	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Desarrollo	No	8
192.168.29.117	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Desarrollo	No	8

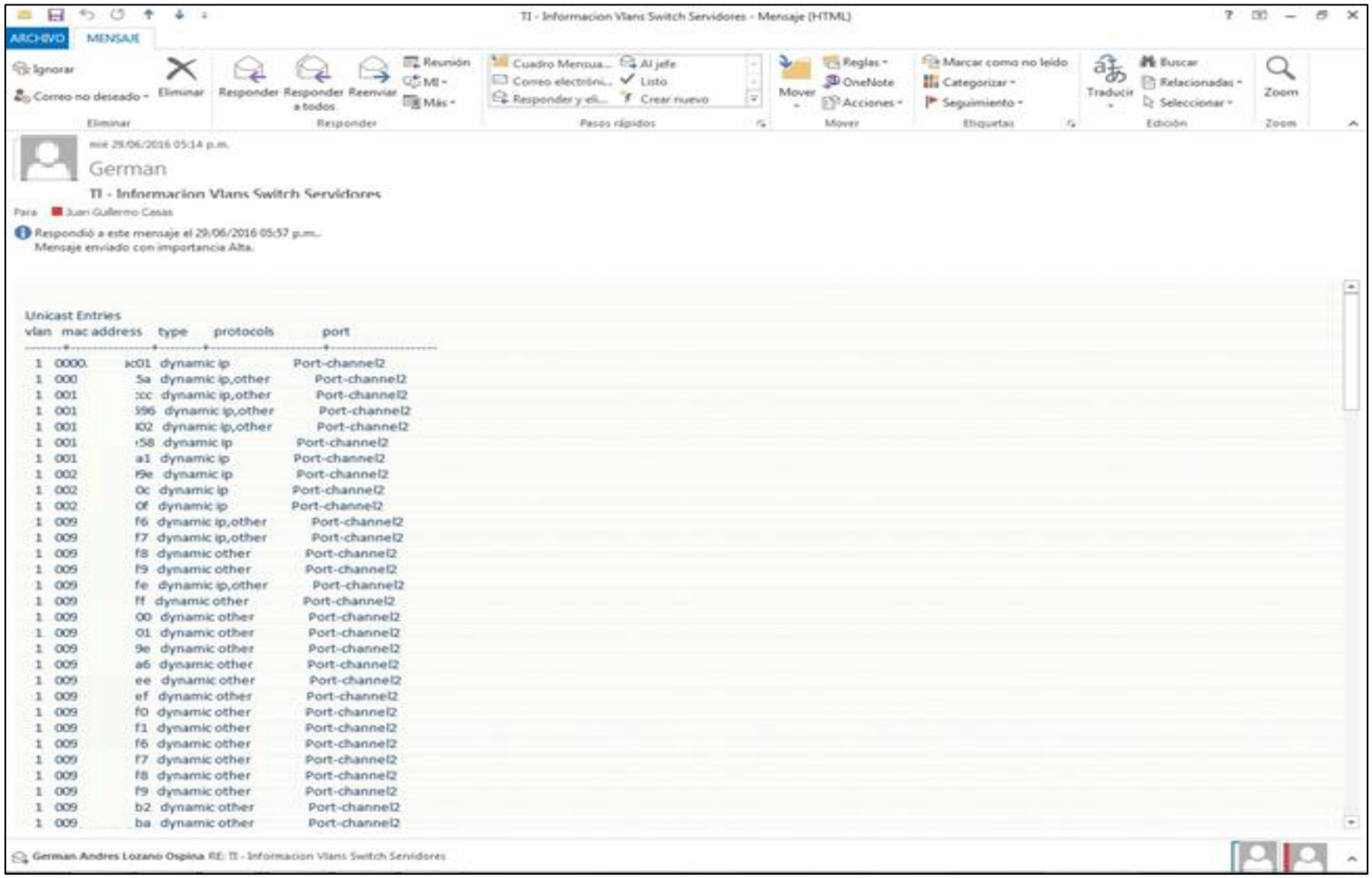
IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.13	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	Pruebas	No	8
192.168.29.82	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Pruebas	No	8
192.168.29.96	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Pruebas	No	8
192.168.29.96	Oracle 9iAS iSQLplus XSS	High	Pruebas	No	8
192.168.29.97	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Pruebas	No	8
192.168.29.26	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Desarrollo	No	8
192.168.29.5	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Pruebas	No	8
192.168.29.68	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Desarrollo	No	8
192.168.29.68	Oracle 9iAS iSQLplus XSS	High	Desarrollo	No	8
192.168.29.33	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Pruebas	No	8
192.168.29.50	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	8
192.168.29.50	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	Desarrollo	No	8
192.168.29.53	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	Pruebas	No	8
192.168.29.60	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	Desarrollo	No	8
192.168.29.64	Oracle 9iAS iSQLplus XSS	High	Pruebas	No	8
192.168.29.70	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	Desarrollo	No	8
192.168.29.51	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	Desarrollo	No	8
192.168.29.7	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	Pruebas	No	8
192.168.29.125	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Pruebas	No	9
192.168.29.125	OpenSSL < 0.9.8k Denial of Service	Medium	Pruebas	No	9
192.168.29.18	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	9
192.168.29.18	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Pruebas	No	9
192.168.29.18	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	9
192.168.29.25	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	9
192.168.29.34	OpenSSL < 0.9.8y Multiple Vulnerabilities	Medium	Desarrollo	No	9
192.168.29.38	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	9
192.168.29.40	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium	Desarrollo	No	9
192.168.29.71	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	Desarrollo	No	9
192.168.29.71	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Desarrollo	No	9

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.41	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	Pruebas	No	9
192.168.29.41	OpenSSL < 0.9.8i Denial of Service	Medium	Pruebas	No	9
192.168.29.68	OpenSSL < 0.9.8i Denial of Service	Medium	Desarrollo	No	9
192.168.29.73	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	9
192.168.29.27	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Desarrollo	No	9
192.168.29.27	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Desarrollo	No	9
192.168.29.27	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	9
192.168.29.27	OpenSSL < 0.9.6k Denial of Service	Medium	Desarrollo	No	9
192.168.29.31	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	Desarrollo	No	9
192.168.29.31	OpenSSL < 0.9.6k Denial of Service	Medium	Desarrollo	No	9
192.168.29.31	Web Server Expect Header XSS	Medium	Desarrollo	No	9
192.168.29.35	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	Pruebas	No	9
192.168.29.35	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	9
192.168.29.35	OpenSSL < 0.9.6k Denial of Service	Medium	Pruebas	No	9
192.168.29.35	Web Server Expect Header XSS	Medium	Pruebas	No	9
192.168.29.37	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Pruebas	No	9
192.168.29.39	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	Desarrollo	No	9
192.168.29.48	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	9
192.168.29.79	OpenSSL < 0.9.6f Denial of Service	Medium	Desarrollo	No	9
192.168.29.80	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	Pruebas	No	9
192.168.29.80	OpenSSL < 0.9.6k Denial of Service	Medium	Pruebas	No	9
192.168.29.51	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	Desarrollo	No	9
192.168.29.51	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	Desarrollo	No	9
192.168.29.51	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Desarrollo	No	9
192.168.29.51	Web Server Expect Header XSS	Medium	Desarrollo	No	9
192.168.29.58	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	9
192.168.29.96	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	9
192.168.29.96	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	Pruebas	No	9
192.168.29.96	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	9

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.97	MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	Pruebas	No	9
192.168.29.97	OpenSSL < 0.9.8l Multiple Vulnerabilities	Medium	Pruebas	No	9
192.168.29.97	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Pruebas	No	9
192.168.29.97	Symantec AntiVirus Detection (Corporate Edition)	Medium	Pruebas	No	9
192.168.29.33	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	Pruebas	No	9
192.168.29.33	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Medium	Pruebas	No	9
192.168.29.7	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)	Medium	Pruebas	No	9
192.168.29.7	OpenSSL < 0.9.8i Denial of Service	Medium	Pruebas	No	9
192.168.29.7	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	Pruebas	No	9
192.168.29.89	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Productivo	Si	No se Gestiona
192.168.29.118	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	Si	No se Gestiona
192.168.29.61	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	Si	No se Gestiona
192.168.29.61	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	Si	No se Gestiona
192.168.29.14	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	Si	No se Gestiona
192.168.29.101	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	Productivo	No	No se Gestiona
192.168.29.101	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Productivo	No	No se Gestiona
192.168.29.56	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	No se Gestiona
192.168.29.56	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Productivo	No	No se Gestiona
192.168.29.16	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	No se Gestiona
192.168.29.30	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	No	No se Gestiona
192.168.29.57	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	No	No se Gestiona
192.168.29.88	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Productivo	No	No se Gestiona
192.168.29.55	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	No se Gestiona
192.168.29.2	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	No se Gestiona
192.168.29.2	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	No	No se Gestiona
192.168.29.59	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	No	No se Gestiona
192.168.29.59	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Productivo	No	No se Gestiona
192.168.29.59	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Productivo	No	No se Gestiona
192.168.29.19	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Productivo	No	No se Gestiona
192.168.29.19	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Productivo	No	No se Gestiona

IP	Vulnerabilidad	Criticidad	Ambiente	Core	Orden Gestión Vulnerabilidades Escenario Actual
192.168.29.19	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Productivo	No	No se Gestiona
192.168.29.25	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Pruebas	No	No se Gestiona
192.168.29.40	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Desarrollo	No	No se Gestiona
192.168.29.71	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Desarrollo	No	No se Gestiona
192.168.29.71	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Desarrollo	No	No se Gestiona
192.168.29.72	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Desarrollo	No	No se Gestiona
192.168.29.81	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Desarrollo	No	No se Gestiona
192.168.29.94	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Pruebas	No	No se Gestiona
192.168.29.12	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Desarrollo	No	No se Gestiona
192.168.29.12	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Desarrollo	No	No se Gestiona
192.168.29.13	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Pruebas	No	No se Gestiona
192.168.29.26	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Desarrollo	No	No se Gestiona
192.168.29.26	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Desarrollo	No	No se Gestiona
192.168.29.41	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Pruebas	No	No se Gestiona
192.168.29.68	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Desarrollo	No	No se Gestiona
192.168.29.70	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Desarrollo	No	No se Gestiona
192.168.29.73	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Pruebas	No	No se Gestiona
192.168.29.27	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)	Low	Desarrollo	No	No se Gestiona
192.168.29.35	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Pruebas	No	No se Gestiona
192.168.29.37	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	Pruebas	No	No se Gestiona
192.168.29.39	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Desarrollo	No	No se Gestiona
192.168.29.39	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Desarrollo	No	No se Gestiona
192.168.29.48	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	Pruebas	No	No se Gestiona
192.168.29.48	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Pruebas	No	No se Gestiona
192.168.29.51	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Desarrollo	No	No se Gestiona
192.168.29.51	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Low	Desarrollo	No	No se Gestiona
192.168.29.51	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Desarrollo	No	No se Gestiona
192.168.29.58	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Pruebas	No	No se Gestiona
192.168.29.96	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Pruebas	No	No se Gestiona
192.168.29.97	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Pruebas	No	No se Gestiona
192.168.29.33	ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	Pruebas	No	No se Gestiona
192.168.29.7	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	Pruebas	No	No se Gestiona
192.168.29.7	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	Pruebas	No	No se Gestiona

ANEXO F
INFORMACIÓN SWITCH



TI - Informacion Vlans Switch Servidores - Mensaje (HTML)

ARCHIVO MENSAJE

Ignorar | Correo no deseado | Eliminar | Responder | Responder a todos | Reenviar | Reunión | Más | Cuadro Mensua... | Correo electróni... | Responder y eli... | Al jefe | Listo | Crear nuevo | Mover | Reglas | OneNote | Acciones | Marcar como no leído | Categorizar | Seguimiento | Traducir | Buscar | Relacionadas | Seleccionar | Zoom

Eliminar | Responder | Pasos rápidos | Mover | Etiquetas | Edición | Zoom

mié 29/06/2016 05:14 p.m.

German

TI - Informacion Vlans Switch Servidores

Para Juan Guillermo Casas

Respondió a este mensaje el 29/06/2016 05:57 p.m..
Mensaje enviado con importancia Alta.

Unicast Entries

vlan	mac address	type	protocols	port
1	0000.	ac01	dynamic	ip Port-channel2
1	000	5a	dynamic	ip,other Port-channel2
1	001	:cc	dynamic	ip,other Port-channel2
1	001	596	dynamic	ip,other Port-channel2
1	001	102	dynamic	ip,other Port-channel2
1	001	:58	dynamic	ip Port-channel2
1	001	a1	dynamic	ip Port-channel2
1	002	f9e	dynamic	ip Port-channel2
1	002	0c	dynamic	ip Port-channel2
1	002	0f	dynamic	ip Port-channel2
1	009	f6	dynamic	ip,other Port-channel2
1	009	f7	dynamic	ip,other Port-channel2
1	009	f8	dynamic	other Port-channel2
1	009	f9	dynamic	other Port-channel2
1	009	fe	dynamic	ip,other Port-channel2
1	009	ff	dynamic	other Port-channel2
1	009	00	dynamic	other Port-channel2
1	009	01	dynamic	other Port-channel2
1	009	9e	dynamic	other Port-channel2
1	009	a6	dynamic	other Port-channel2
1	009	ee	dynamic	other Port-channel2
1	009	ef	dynamic	other Port-channel2
1	009	f0	dynamic	other Port-channel2
1	009	f1	dynamic	other Port-channel2
1	009	f6	dynamic	other Port-channel2
1	009	f7	dynamic	other Port-channel2
1	009	f8	dynamic	other Port-channel2
1	009	f9	dynamic	other Port-channel2
1	009	b2	dynamic	other Port-channel2
1	009	ba	dynamic	other Port-channel2

German Andres Lozano Ospina RE: TI - Informacion Vlans Switch Servidores

ANEXO G
ACTIVOS POR SEGMENTO DE RED

IP	ID Red	SW	MAC
192.168.29.10	1	XYZ	0000.0c07.ac01
192.168.29.101	10	ABC	000d.6083.b882
192.168.29.104	1	XYZ	000c.29ef.045a
192.168.29.117	1	XYZ	0014.5ee0.3ccc
192.168.29.118	1	XYZ	0014.5ee1.3596
192.168.29.12	1	XYZ	0090.fac1.8af6
192.168.29.120	10	ABC	0011.2557.6e89
192.168.29.125	10	ABC	0014.5e3f.1b1d
192.168.29.13	1	XYZ	0090.fac1.8af7
192.168.29.14	1	ABC	0090.fac1.8af8
192.168.29.16	1	ABC	0090.fac1.8af9
192.168.29.18	10	ABC	001a.642f.fde2
192.168.29.19	1	ABC	0090.fac2.72ef
192.168.29.2	10	ABC	001c.7f3f.9267
192.168.29.21	1	ABC	0090.fac2.72f0
192.168.29.23	10	ABC	001c.c4a8.7f4c
192.168.29.24	10	ABC	0050.5688.6671
192.168.29.25	10	ABC	0050.5690.0be5
192.168.29.26	10	XYZ	0050.5690.0f78
192.168.29.27	1	ABC	0090.fac2.72f1
192.168.29.30	1	ABC	0090.fac2.72f6
192.168.29.31	1	ABC	0090.fac2.72f7
192.168.29.33	10	XYZ	0050.5690.274e
192.168.29.34	1	ABC	0090.fac2.72f8
192.168.29.35	1	ABC	0090.fac2.72f9
192.168.29.37	1	ABC	0090.fac2.73b2
192.168.29.38	1	ABC	1803.730a.2ccc
192.168.29.39	1	ABC	1803.730a.2d26
192.168.29.40	1	ABC	1803.730a.2ec3
192.168.29.41	10	XYZ	0050.56b0.38ea
192.168.29.43	1	ABC	64a0.e743.c7c3
192.168.29.46	9	DEF	0050.5682.42ec
192.168.29.47	1	ABC	64a0.e743.fc43
192.168.29.48	1	ABC	90e2.ba94.c808

IP	ID Red	SW	MAC
192.168.29.49	1	DEF	c84c.7598.3d3f
192.168.29.5	10	XYZ	0050.56b0.60dd
192.168.29.50	1	DEF	e41f.1332.6ee8
192.168.29.51	1	DEF	f04d.a2d9.d2aa
192.168.29.53	1	DEF	f04d.a2d9.d2af
192.168.29.55	2	XYZ	0000.0c07.ac14
192.168.29.56	2	XYZ	0000.0c07.ac1e
192.168.29.57	2	XYZ	7426.ac05.0100
192.168.29.58	9	DEF	0050.5682.42ee
192.168.29.59	10	XYZ	0050.56b0.7e26
192.168.29.60	2	DEF	7426.ac05.1500
192.168.29.61	10	XYZ	0050.56bd.0007
192.168.29.63	2	DEF	f44e.05e9.0f01
192.168.29.64	2	DEF	f44e.05e9.1001
192.168.29.68	10	XYZ	0050.56bd.0013
192.168.29.69	10	XYZ	0050.56bd.0017
192.168.29.7	3	XYZ	0000.0c07.ac1f
192.168.29.70	3	XYZ	0000.0c07.ac28
192.168.29.71	3	ABC	fc5b.39cd.4c00
192.168.29.72	3	ABC	fc5b.39cd.6600
192.168.29.73	9	XYZ	0000.0000.4b00
192.168.29.76	9	XYZ	0000.0000.4b01
192.168.29.77	9	XYZ	001a.6434.13ae
192.168.29.78	9	ABC	001a.648b.2e9e
192.168.29.79	9	ABC	001a.648b.6316
192.168.29.80	9	ABC	001a.6494.f834
192.168.29.81	9	ABC	001a.6496.dcdf
192.168.29.82	9	DEF	0021.5e9b.e458
192.168.29.84	10	XYZ	0050.56bd.004f
192.168.29.88	9	DEF	0021.5ec2.7780
192.168.29.89	9	DEF	0050.56b0.0740
192.168.29.93	9	DEF	0021.5ec2.7781
192.168.29.94	9	DEF	0021.5ec5.2b6c
192.168.29.95	9	DEF	0021.5ef9.9e2c
192.168.29.96	9	DEF	0050.56b0.23e2
192.168.29.97	9	DEF	0021.5ef9.9e2d

VALORACIÓN ACTIVOS POR TIPO DE INFORMACIÓN VS NORMATIVIDAD

IP	Ambiente	Core	Tipo de Información	Normatividad	Valoración
192.168.29.56	Productivo	No	9	9	9
192.168.29.89	Productivo	Si	7	9	9
192.168.29.43	Productivo	No	7	9	9
192.168.29.118	Productivo	Si	7	9	9
192.168.29.101	Productivo	No	9	9	9
192.168.29.47	Productivo	Si	7	9	9
192.168.29.49	Productivo	No	5	9	6
192.168.29.24	Productivo	Si	9	9	9
192.168.29.84	Productivo	Si	7	6	7
192.168.29.77	Productivo	No	7	6	7
192.168.29.21	Productivo	No	9	6	8
192.168.29.61	Productivo	Si	7	9	9
192.168.29.55	Productivo	No	7	6	7
192.168.29.14	Productivo	Si	7	6	7
192.168.29.88	Productivo	No	7	6	7
192.168.29.16	Productivo	No	9	1	8
192.168.29.57	Productivo	No	9	1	8
192.168.29.69	Productivo	No	9	1	8
192.168.29.76	Productivo	No	7	1	8
192.168.29.72	Desarrollo	No	5	1	2
192.168.29.60	Desarrollo	No	5	1	2
192.168.29.13	Pruebas	No	5	1	2
192.168.29.94	Pruebas	No	5	1	2
192.168.29.59	Productivo	No	5	1	2
192.168.29.68	Desarrollo	No	5	1	2
192.168.29.64	Pruebas	No	5	1	2
192.168.29.10	Desarrollo	No	5	1	2
192.168.29.104	Desarrollo	No	5	1	2
192.168.29.5	Pruebas	No	5	1	2
192.168.29.78	Productivo	No	5	1	2
192.168.29.81	Desarrollo	No	5	1	2
192.168.29.34	Desarrollo	No	5	1	2
192.168.29.120	Productivo	No	7	1	8

IP	Ambiente	Core	Tipo de Información	Normatividad	Valoración
192.168.29.23	Productivo	No	7	1	8
192.168.29.70	Desarrollo	No	5	1	2
192.168.29.38	Desarrollo	No	5	1	2
192.168.29.30	Productivo	No	7	1	8
192.168.29.19	Productivo	No	3	1	1
192.168.29.27	Desarrollo	No	3	1	1
192.168.29.35	Pruebas	No	3	1	1
192.168.29.37	Pruebas	No	3	1	1
192.168.29.48	Pruebas	No	3	1	1
192.168.29.51	Desarrollo	No	3	1	1
192.168.29.82	Pruebas	No	3	1	1
192.168.29.18	Pruebas	No	5	1	2
192.168.29.26	Desarrollo	No	5	1	2
192.168.29.93	Desarrollo	No	5	1	2
192.168.29.63	Pruebas	No	5	1	2
192.168.29.125	Pruebas	No	5	1	2
192.168.29.25	Pruebas	No	5	1	2
192.168.29.71	Desarrollo	No	5	1	2
192.168.29.117	Desarrollo	No	5	1	2
192.168.29.46	Productivo	No	5	1	2
192.168.29.40	Desarrollo	No	5	1	2
192.168.29.50	Desarrollo	No	5	1	2
192.168.29.53	Pruebas	No	5	1	2
192.168.29.12	Desarrollo	No	5	1	2
192.168.29.96	Pruebas	No	3	1	1
192.168.29.97	Pruebas	No	3	1	1
192.168.29.7	Pruebas	No	3	1	1
192.168.29.79	Desarrollo	No	3	1	1
192.168.29.80	Pruebas	No	3	1	1
192.168.29.31	Desarrollo	No	3	1	1
192.168.29.41	Pruebas	No	5	1	2
192.168.29.2	Productivo	No	5	1	2
192.168.29.95	Productivo	No	3	1	1
192.168.29.73	Pruebas	No	5	1	2
192.168.29.39	Desarrollo	No	3	1	1
192.168.29.58	Pruebas	No	3	1	1
192.168.29.33	Pruebas	No	3	1	1

ANEXO H
CERTIFICACIÓN BANCO DE OCCIDENTE

Banco de Occidente

Bogotá D.C., 30 de Agosto de 2017

Señores
Universidad Piloto de Colombia
Dirección de Posgrados especialización seguridad Informática
Bogotá

Respetados señores.

Por solicitud de los interesados, manifiesto que luego de haber recibido el documento y analizado la "Metodología para la optimización en la gestión de vulnerabilidades en Banco de Occidente" desarrollada por los ingenieros David Fernando Ramirez Leon y Juan Guillermo Casas Pinto, encontramos que los objetivos que allí se persiguen, pueden aportar en el futuro cercano, un gran valor para nuestra estrategia de gestión de vulnerabilidades, así mismo, la metodología planteada puede ser incorporada a nuestros procesos de forma integral.

Agradezco mucho su amable atención.

Cordialmente

Victor Yuxon Yomayusa Agredo
Director Seguricad Informática
Banco de Occidente
Celular 3002097769

ANEXO I
CERTIFICACIÓN BANCO DE OCCIDENTE

De: Daniel Infante Godoy
Para: David Fernando Ramirez Leon
CC:
Asunto: RE: Documento de Metodologia vulnerabilidades propuetsa
Enviado el: martes 29/08/2017 14:30

De: Daniel Infante Godoy
Enviado el: martes, 15 de agosto de 2017 10:10 p.m.
Para: Victor Yuxon Yomayusa Agredo
Asunto: RV: Documento de Metodologia vulnerabilidades propuetsa

Buenas noches.

Victor, revisando el documento enviado por David en referencia a la metodología propuesta para la gestión de vulnerabilidades, encuentro que los objetivos que evaluamos en el proyecto se cumplen satisfactoriamente, la clasificación de activos realizada así como la formulación propuesta para integrar la criticidad de los activos de información con la criticidad de las vulnerabilidades encontradas en ellos y, su relación transversal con activos del mismo entorno, ofrece una solución aplicable a la siguiente fase en el proceso de la gestión las vulnerabilidades.

Banco de Occidente

Daniel Infante Godoy
Ingeniero de Seguridad Informática | Gerencia de Tecnología
Vicepresidencia de Operaciones y Tecnología

Tel: (1) 756 0999 - 17789 - DG Bogotá
Email: Dinfante@bancodeoccidente.com.co
www.bancodeoccidente.com.co

/BcoOccidente @bco_occidente /banco-de-occidente @Bco_Occidente @Bco_OccidenteMD

ANEXO J
DATOS METODOLOGÍA PROPUESTA

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.47	ABC	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	9	Productivo	Si	9	9	81	272	353	362	1	Critico	1
192.168.29.47	ABC	1	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	9	Productivo	Si	9	9	81	272	353	362	1	Critico	2
192.168.29.47	ABC	1	Windows Service Pack Out-of-Date	Critical	9	Productivo	Si	9	9	81	272	353	362	1	Critico	3
192.168.29.101	ABC	10	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	4
192.168.29.101	ABC	10	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	5
192.168.29.101	ABC	10	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	6
192.168.29.101	ABC	10	Windows Service Pack Out-of-Date	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	7
192.168.29.48	ABC	1	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	8
192.168.29.48	ABC	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	9
192.168.29.48	ABC	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	10
192.168.29.48	ABC	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	11
192.168.29.48	ABC	1	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	12
192.168.29.48	ABC	1	OpenSSL c09 &l Denial of Service	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	13
192.168.29.48	ABC	1	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	9	Productivo	No	0	9	81	272	353	353	4	Critico	14
192.168.29.120	ABC	10	MS09-050: Microsoft Windows SMB2 Smb2Validate Provide Callback) Vulnerability (975497) (uncredentialed check)	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	15
192.168.29.120	ABC	10	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	16
192.168.29.120	ABC	10	OpenSSL c09 &l Denial of Service	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	17
192.168.29.120	ABC	10	OpenSSL c09 &h Multiple Vulnerabilities	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	18
192.168.29.120	ABC	10	OpenSSL c09 &j Signature Spoofing	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	19

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.120	ABC	10	Windows Service PackOut-of-Date	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	20
192.168.29.16	ABC	1	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	21
192.168.29.21	ABC	1	MS15-021: Security Update for Schannel to Address Spoofing (3061320)	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	22
192.168.29.23	ABC	10	OpenSSL c09.61 Denial of Service	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	23
192.168.29.23	ABC	10	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Productivo	No	0	8	72	272	344	344	4	Critico	24
192.168.29.24	ABC	10	OpenSSL c09.8 u Multiple Vulnerabilities	High	7	Productivo	Si	9	9	63	272	335	344	2	Critico	25
192.168.29.47	ABC	1	Apache c 13.3 1/2.0.48 Socket Connection Blocking Race Condition DoS	High	7	Productivo	Si	9	9	63	272	335	344	2	Critico	26
192.168.29.47	ABC	1	Apache 2.2.x c2.2.27 Multiple Vulnerabilities	High	7	Productivo	Si	9	9	63	272	335	344	2	Critico	27
192.168.29.47	ABC	1	Oracle 9iAS ISQLplus XSS	High	7	Productivo	Si	9	9	63	272	335	344	2	Critico	28
192.168.29.47	ABC	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Productivo	Si	9	9	63	272	335	344	2	Critico	29
192.168.29.14	ABC	1	ESXi 5.5 c Build 1623387 Multiple Vulnerabilities (remote check)	Critical	9	Productivo	Si	7	7	63	272	335	342	1	Critico	30
192.168.29.101	ABC	10	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	7	Productivo	No	0	9	63	272	335	335	5	Critico	31
192.168.29.101	ABC	10	OpenSSL 0.9.8 c 0.9.8x DTLS CBC Denial of Service	High	7	Productivo	No	0	9	63	272	335	335	5	Critico	32
192.168.29.48	ABC	1	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Productivo	No	0	9	63	272	335	335	5	Critico	33
192.168.29.48	ABC	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Productivo	No	0	9	63	272	335	335	5	Critico	34
192.168.29.21	ABC	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Productivo	No	0	8	56	272	328	328	5	Critico	35
192.168.29.125	ABC	10	OpenSSL c09.6 m/ 0.9.7d Denial of Service	Critical	9	Pruebas	No	0	2	18	272	290	290	7	Critico	36
192.168.29.18	ABC	10	MS09-050: Microsoft Windows SMB Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	9	Pruebas	No	0	2	18	272	290	290	7	Critico	37
192.168.29.18	ABC	10	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Pruebas	No	0	2	18	272	290	290	7	Critico	38

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V..x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V..x LAN) +Si es core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.18	ABC	10	OpenSSL c09 &l Denial of Service	Critical	9	Pruebas	No	0	2	18	272	290	290	7	Critico	39
192.168.29.25	ABC	10	ESXi 5.5 c Build 1623387 Multiple Vulnerabilities (remote check)	Critical	9	Pruebas	No	0	2	18	272	290	290	7	Critico	40
192.168.29.34	ABC	1	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical	9	Desarrollo	No	0	2	18	272	290	290	7	Critico	41
192.168.29.34	ABC	1	OpenSSL c09 &l Denial of Service	Critical	9	Desarrollo	No	0	2	18	272	290	290	7	Critico	42
192.168.29.33	ABC	1	OpenSSL c09 &m/ 0.9.7d Denial of Service	Critical	9	Desarrollo	No	0	2	18	272	290	290	7	Critico	43
192.168.29.40	ABC	1	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	9	Desarrollo	No	0	2	18	272	290	290	7	Critico	44
192.168.29.125	ABC	10	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Pruebas	No	0	2	14	272	286	286	8	Critico	45
192.168.29.18	ABC	10	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	7	Pruebas	No	0	2	14	272	286	286	8	Critico	46
192.168.29.18	ABC	10	OpenSSL c09 &u Multiple Vulnerabilities	High	7	Pruebas	No	0	2	14	272	286	286	8	Critico	47
192.168.29.18	ABC	10	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Pruebas	No	0	2	14	272	286	286	8	Critico	48
192.168.29.25	ABC	10	OpenSSL 0.9.8 c0.9.8x DTLS CBC Denial of Service	High	7	Pruebas	No	0	2	14	272	286	286	8	Critico	49
192.168.29.33	ABC	1	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	7	Desarrollo	No	0	2	14	272	286	286	8	Critico	50
192.168.29.19	ABC	1	Apache 2.2.x <2.2.23 Multiple Vulnerabilities	Critical	9	Productivo	No	0	1	9	272	281	281	4	Critico	51
192.168.29.19	ABC	1	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	1	9	272	281	281	4	Critico	52
192.168.29.19	ABC	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Critical	9	Productivo	No	0	1	9	272	281	281	4	Critico	53
192.168.29.19	ABC	1	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	9	Productivo	No	0	1	9	272	281	281	4	Critico	54
192.168.29.27	ABC	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	9	Desarrollo	No	0	1	9	272	281	281	7	Critico	55
192.168.29.27	ABC	1	Windows Service Pack Out-of-Date	Critical	9	Desarrollo	No	0	1	9	272	281	281	7	Critico	56
192.168.29.35	ABC	1	Apache 2.2.x <2.2.23 Multiple Vulnerabilities	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	57

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Si es core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.35	ABC	1	Microsoft SQL Server Unsupported Version Detection	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	58
192.168.29.35	ABC	1	MS09-050: Microsoft Windows SMB2 Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	59
192.168.29.35	ABC	1	OpenSSL c09.8h Multiple Vulnerabilities	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	60
192.168.29.37	ABC	1	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	61
192.168.29.37	ABC	1	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	62
192.168.29.37	ABC	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	63
192.168.29.37	ABC	1	OpenSSL c09.8l Denial of Service	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	64
192.168.29.43	ABC	1	ESXi 5.5 c Build 1623387 Multiple Vulnerabilities (remote check)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	65
192.168.29.43	ABC	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	66
192.168.29.43	ABC	1	MS13-052: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2848295)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	67
192.168.29.43	ABC	1	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	68
192.168.29.43	ABC	1	OpenSSL c09.6m/0.9.7d Denial of Service	Critical	9	Pruebas	No	0	1	9	272	281	281	7	Critico	69
192.168.29.19	ABC	1	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Productivo	No	0	1	7	272	279	279	3	Critico	70
192.168.29.27	ABC	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Desarrollo	No	0	1	7	272	279	279	8	Critico	71
192.168.29.35	ABC	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Pruebas	No	0	1	7	272	279	279	8	Critico	72
192.168.29.37	ABC	1	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Pruebas	No	0	1	7	272	279	279	8	Critico	73
192.168.29.43	ABC	1	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Pruebas	No	0	1	7	272	279	279	8	Critico	74
192.168.29.15	XYZ	2	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	9	81	157	238	238	4	Critico	75
192.168.29.15	XYZ	2	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	9	Productivo	No	0	9	81	157	238	238	4	Critico	76

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V.TipoInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V.TipoInf Vs Normat) + V.x LAN) +Sies core	Orden Gestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.57	XYZ	2	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)	Critical	9	Productivo	No	0	8	72	157	229	229	4	Crítico	77
192.168.29.57	XYZ	2	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Productivo	No	0	8	72	157	229	229	4	Crítico	78
192.168.29.57	XYZ	2	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Productivo	No	0	8	72	157	229	229	4	Crítico	79
192.168.29.55	XYZ	2	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	7	63	157	220	220	4	Crítico	80
192.168.29.56	XYZ	2	MS09-074: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	7	Productivo	No	0	9	63	157	220	220	3	Crítico	81
192.168.29.57	XYZ	2	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Productivo	No	0	8	56	157	213	213	3	Crítico	82
192.168.29.57	XYZ	2	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Productivo	No	0	8	56	157	213	213	3	Crítico	83
192.168.29.89	DEF	9	OpenSSL < 0.9.6m/0.9.7d Denial of Service	Critical	9	Productivo	Si	9	9	81	78	159	168	1	Crítico	84
192.168.29.89	DEF	9	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Productivo	Si	9	9	81	78	159	168	1	Crítico	85
192.168.29.118	XYZ	1	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	9	Productivo	Si	9	9	81	72	153	162	1	Crítico	86
192.168.29.118	XYZ	1	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	9	Productivo	Si	9	9	81	72	153	162	1	Crítico	87
192.168.29.89	DEF	9	Apache < 1.3.31/2.0.48 Socket Connection Blocking Race Condition DoS	High	7	Productivo	Si	9	9	63	78	141	150	2	Crítico	88
192.168.29.61	XYZ	10	OpenSSL < 0.9.6j/0.9.7b Multiple Vulnerabilities	Critical	9	Productivo	Si	9	9	81	57	138	147	1	Crítico	89
192.168.29.118	XYZ	1	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Productivo	Si	9	9	63	72	135	144	2	Crítico	90
192.168.29.88	DEF	9	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	9	Productivo	No	0	7	63	78	141	141	4	Crítico	91
192.168.29.88	DEF	9	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Productivo	No	0	7	63	78	141	141	4	Crítico	92
192.168.29.69	XYZ	10	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	8	72	57	129	129	4	Crítico	93
192.168.29.84	XYZ	10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Crítico	94
192.168.29.84	XYZ	10	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Crítico	95

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipoInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipoInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.69	XYZ	10	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Productivo	No	0	8	56	57	113	113	3	Critico	96
192.168.29.46	DEF	9	OpenSSL < 0.9.8j / 0.9.7b Multiple Vulnerabilities	Critical	9	Productivo	No	0	2	18	78	96	96	4	Alto	97
192.168.29.46	DEF	9	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	9	Productivo	No	0	2	18	78	96	96	4	Alto	98
192.168.29.46	DEF	9	Unsupported Unix Operating System	Critical	9	Productivo	No	0	2	18	78	96	96	4	Alto	99
192.168.29.93	DEF	9	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Desarrollo	No	0	2	18	78	96	96	7	Alto	100
192.168.29.94	DEF	9	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	9	Pruebas	No	0	2	18	78	96	96	7	Alto	101
192.168.29.94	DEF	9	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Pruebas	No	0	2	18	78	96	96	7	Alto	102
192.168.29.94	DEF	9	OpenSSL < 0.9.8j Signature Spoofing	Critical	9	Pruebas	No	0	2	18	78	96	96	7	Alto	103
192.168.29.93	DEF	9	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	7	Desarrollo	No	0	2	14	78	92	92	8	Alto	104
192.168.29.93	DEF	9	Oracle 9iAS SQLplus XSS	High	7	Desarrollo	No	0	2	14	78	92	92	8	Alto	105
192.168.29.93	DEF	9	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Desarrollo	No	0	2	14	78	92	92	8	Alto	106
192.168.29.10	XYZ	1	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	107
192.168.29.10	XYZ	1	Unsupported Unix Operating System	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	108
192.168.29.104	XYZ	1	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	109
192.168.29.104	XYZ	1	MS15-031: Security Update for Schannel to Address Spoofing (3081320)	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	110
192.168.29.104	XYZ	1	OpenSSL < 0.9.6l Denial of Service	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	111
192.168.29.104	XYZ	1	Windows Service Pack Out-of-Date	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	112
192.168.29.12	XYZ	1	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	113
192.168.29.12	XYZ	1	OpenSSL < 0.9.6l Denial of Service	Critical	9	Desarrollo	No	0	2	18	72	90	90	7	Alto	114
192.168.29.118	XYZ	1	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Productivo	Si	9	9	63	72	135	144	2	Critico	90
192.168.29.88	DEF	9	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	9	Productivo	No	0	7	63	78	141	141	4	Critico	91
192.168.29.88	DEF	9	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Productivo	No	0	7	63	78	141	141	4	Critico	92
192.168.29.69	XYZ	10	Microsoft SQL Server Unsupported Version Detection	Critical	9	Productivo	No	0	8	72	57	129	129	4	Critico	93
192.168.29.84	XYZ	10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Critico	94
192.168.29.84	XYZ	10	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Critico	95

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipoInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipoInf Vs Normat) + V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.18	XYZ	1	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution [975517]	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	115
192.168.29.18	XYZ	1	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution [982214]	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	116
192.168.29.18	XYZ	1	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution [2733594]	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	117
192.168.29.18	XYZ	1	MS13-052: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege [2849470]	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	118
192.168.29.18	XYZ	1	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	119
192.168.29.18	XYZ	1	Unsupported Unix Operating System	Critical	9	Pruebas	No	0	2	18	72	90	90	7	Alto	120
192.168.29.58	DEF	9	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution [982214] (remote check)	Critical	9	Pruebas	No	0	1	9	78	87	87	7	Alto	121
192.168.29.58	DEF	9	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege [2958732]	Critical	9	Pruebas	No	0	1	9	78	87	87	7	Alto	122
192.168.29.82	DEF	9	OpenSSL c09.6m/ 0.9.7d Denial of Service	Critical	9	Pruebas	No	0	1	9	78	87	87	7	Alto	123
192.168.29.95	DEF	9	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege [2958732]	Critical	9	Productivo	No	0	1	9	78	87	87	4	Alto	124
192.168.29.104	XYZ	1	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Desarrollo	No	0	2	14	72	86	86	8	Alto	125
192.168.29.104	XYZ	1	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	7	Desarrollo	No	0	2	14	72	86	86	8	Alto	126
192.168.29.104	XYZ	1	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Desarrollo	No	0	2	14	72	86	86	8	Alto	127
192.168.29.117	XYZ	1	Apache < 1.3.31 / 2.0.48 Socket Connection Blocking Race Condition DoS	High	7	Desarrollo	No	0	2	14	72	86	86	8	Alto	128
192.168.29.18	XYZ	1	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution [974318]	High	7	Pruebas	No	0	2	14	72	86	86	8	Alto	129
192.168.29.82	DEF	9	Apache < 1.3.31 / 2.0.48 Socket Connection Blocking Race Condition DoS	High	7	Pruebas	No	0	1	7	78	85	85	8	Alto	130
192.168.29.96	DEF	9	OpenSSL c09.8u Multiple Vulnerabilities	High	7	Pruebas	No	0	1	7	78	85	85	8	Alto	131
192.168.29.96	DEF	9	Oracle 9iAS ISQLplus XSS	High	7	Pruebas	No	0	1	7	78	85	85	8	Alto	132
192.168.29.97	DEF	9	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Pruebas	No	0	1	7	78	85	85	8	Alto	133
192.168.29.84	XYZ	10	[3105872]	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Critico	95

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (Valor Criticidad x Valoración Tipo Inf Vs Normat)	Valoración por VLAN	Suma (V. Crit. x V. TipInf Vs Normat) + V. x LAN	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.76	XYZ	9	Oracle 9iAS iSQLplus XSS	High	7	Productivo	No	0	8	56	23	79	79	5	Alto	134
192.168.29.26	XYZ	10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	135
192.168.29.26	XYZ	10	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	136
192.168.29.26	XYZ	10	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	137
192.168.29.26	XYZ	10	Oracle Database Unsupported	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	138
192.168.29.26	XYZ	10	Windows Service Pack Out-of-Date	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	139
192.168.29.5	XYZ	10	ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)	Critical	9	Pruebas	No	0	2	18	57	75	75	7	Alto	140
192.168.29.5	XYZ	10	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	9	Pruebas	No	0	2	18	57	75	75	7	Alto	141
192.168.29.59	XYZ	10	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	142
192.168.29.59	XYZ	10	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	143
192.168.29.59	XYZ	10	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	144
192.168.29.59	XYZ	10	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	145
192.168.29.59	XYZ	10	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	146
192.168.29.59	XYZ	10	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	9	Productivo	No	0	2	18	57	75	75	4	Alto	147
192.168.29.68	XYZ	10	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	148
192.168.29.68	XYZ	10	Microsoft SQL Server Unsupported Version Detection	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	149
192.168.29.68	XYZ	10	MS15-121: Security Update for Schannel to Address Spoofing (3081320)	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	150
192.168.29.68	XYZ	10	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	151
192.168.29.68	XYZ	10	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	9	Desarrollo	No	0	2	18	57	75	75	7	Alto	152

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (Valor Criticidad x Valoración Tipo Inf Vs Normat)	Valoración por VLAN	Suma (V. Crit. x V. TipInf Vs Normat) + V. x LAN	Suma ((V. Crit. x V. TipInf Vs Normat) + V. x LAN) + Si es core	Orden Gestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	Orden Gestión Vulnerabilidades Escenario Propuesto
192.168.29.77	XYZ	9	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	7	Productivo	No	0	7	49	23	72	72	5	Alto	153
192.168.29.26	XYZ	10	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service	High	7	Desarrollo	No	0	2	14	57	71	71	8	Alto	154
192.168.29.5	XYZ	10	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Pruebas	No	0	2	14	57	71	71	8	Alto	155
192.168.29.59	XYZ	10	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Productivo	No	0	2	14	57	71	71	5	Alto	156
192.168.29.68	XYZ	10	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS	High	7	Desarrollo	No	0	2	14	57	71	71	8	Alto	157
192.168.29.68	XYZ	10	Oracle 9iAS iSQLplus XSS	High	7	Desarrollo	No	0	2	14	57	71	71	8	Alto	158
192.168.29.33	XYZ	10	OpenSSL < 0.9.6l Denial of Service	Critical	9	Pruebas	No	0	1	9	57	66	66	7	Alto	159
192.168.29.33	XYZ	10	OpenSSL < 0.9.8j Signature Spoofing	Critical	9	Pruebas	No	0	1	9	57	66	66	7	Alto	160
192.168.29.33	XYZ	10	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Pruebas	No	0	1	7	57	64	64	8	Alto	161
192.168.29.49	DEF	1	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)	Critical	9	Productivo	No	0	6	54	0	54	54	4	Alto	162
192.168.29.49	DEF	1	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)	Critical	9	Productivo	No	0	6	54	0	54	54	4	Alto	163
192.168.29.49	DEF	1	OpenSSL < 0.9.6m / 0.9.7d Denial of Service	Critical	9	Productivo	No	0	6	54	0	54	54	4	Alto	164
192.168.29.24	ABC	10	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	165
192.168.29.24	ABC	10	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	166
192.168.29.24	ABC	10	OpenSSL < 0.9.8i Denial of Service	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	167
192.168.29.47	ABC	1	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	168
192.168.29.47	ABC	1	OpenSSL < 0.9.8i Denial of Service	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	169
192.168.29.47	ABC	1	Web Server Expect Header XSS	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	170
192.168.29.118	XYZ	1	ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	171

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V.x LAN) +Sis core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.112	XYZ	1	MS09-012: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	172
192.168.29.112	XYZ	1	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	173
192.168.29.112	XYZ	1	MS13-015: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822538)	Medium	5	Productivo	Si	9	9	45	0	45	54	3	Alto	174
192.168.29.101	ABC	10	MS11-074: Vulnerabilities in Microsoft Share Point Could Allow Elevation of Privilege (2451858)	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	175
192.168.29.101	ABC	10	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	176
192.168.29.101	ABC	10	OpenSSL ccs 2 Week Default Configuration	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	177
192.168.29.101	ABC	10	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	178
192.168.29.56	XYZ	2	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	179
192.168.29.56	XYZ	2	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	5	Productivo	No	0	9	45	0	45	45	6	Alto	180
192.168.29.48	DEF	1	Apache c 13 3 1/2 0 48 Socket Connection Blocking Race Condition DoS	High	7	Productivo	No	0	6	42	0	42	42	5	Medio	181
192.168.29.48	DEF	1	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	High	7	Productivo	No	0	6	42	0	42	42	5	Medio	182
192.168.29.14	ABC	1	OpenSSL ccs 2 Week Default Configuration	Medium	5	Productivo	Si	7	7	35	0	35	42	3	Medio	183
192.168.29.73	XYZ	9	ESXi 5.5 c Build 1623387 Multiple Vulnerabilities (remote check)	Critical	9	Pruebas	No	0	2	18	23	41	41	7	Medio	184
192.168.29.120	ABC	10	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	185
192.168.29.120	ABC	10	MS12-011: Vulnerabilities in Microsoft Share Point Could Allow Elevation of Privilege (2663841)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	186
192.168.29.120	ABC	10	OpenSSL ccs 6 f Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	187
192.168.29.120	ABC	10	OpenSSL ccs 6 k Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	188
192.168.29.120	ABC	10	OpenSSL ccs 8 i Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	189
192.168.29.120	ABC	10	OpenSSL ccs 8 y Multiple Vulnerabilities	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	190
192.168.29.84	XYZ	10	(3105872)	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Critico	95

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipoInf Vs Normat) +V.x LAN	Suma ((V.Crit.x V. TipoInf Vs Normat) +V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.16	ABC	1	Symantec AntiVirus Detection (Corporate Edition)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	191
192.168.29.21	ABC	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	192
192.168.29.21	ABC	1	OpenSSL 0.9.6f Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	193
192.168.29.23	ABC	10	MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	194
192.168.29.23	ABC	10	OpenSSL 0.9.8k Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	195
192.168.29.30	ABC	1	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	196
192.168.29.30	ABC	1	MS13-055: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822538)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	197
192.168.29.57	XYZ	2	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	198
192.168.29.57	XYZ	2	MS12-011: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	199
192.168.29.57	XYZ	2	OpenSSL 0.9.6f Denial of Service	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	200
192.168.29.57	XYZ	2	OpenSSL 0.9.8y Multiple Vulnerabilities	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	201
192.168.29.76	XYZ	9	MS13-055: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822538)	Medium	5	Productivo	No	0	8	40	0	40	40	6	Medio	202
192.168.29.89	DEF	9	ESXi 5.5 c Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Productivo	Si	9	9	27	0	27	36	No es gestiona	Medio	203
192.168.29.118	XYZ	1	Apache 2.2.x <2.2.24 Multiple XSS Vulnerabilities	Low	3	Productivo	Si	9	9	27	0	27	36	No es gestiona	Medio	204
192.168.29.61	XYZ	10	Apache 2.2.x <2.2.24 Multiple XSS Vulnerabilities	Low	3	Productivo	Si	9	9	27	0	27	36	No es gestiona	Medio	205
192.168.29.61	XYZ	10	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2689502)	Low	3	Productivo	Si	9	9	27	0	27	36	No es gestiona	Medio	206
192.168.29.88	DEF	9	MS09-012: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	5	Productivo	No	0	7	35	0	35	35	6	Medio	207
192.168.29.88	DEF	9	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Productivo	No	0	7	35	0	35	35	6	Medio	208
192.168.29.88	DEF	9	OpenSSL 0.9.8 Weak Default Configuration	Medium	5	Productivo	No	0	7	35	0	35	35	6	Medio	209
192.168.29.84	XYZ	10	(3105872)	Critical	9	Productivo	Si	7	7	63	57	120	127	1	Critico	93

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipoInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipoInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.48	DEF	1	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Productivo	No	0	6	30	0	30	30	6	Medio	210
192.168.29.14	ABC	1	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Productivo	Si	7	7	21	0	21	28	No se gestiona	Medio	211
192.168.29.101	ABC	10	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Low	3	Productivo	No	0	9	27	0	27	27	No se gestiona	Medio	212
192.168.29.101	ABC	10	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Productivo	No	0	9	27	0	27	27	No se gestiona	Medio	213
192.168.29.55	XYZ	2	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Productivo	No	0	9	27	0	27	27	No se gestiona	Medio	214
192.168.29.55	XYZ	2	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Low	3	Productivo	No	0	9	27	0	27	27	No se gestiona	Medio	215
192.168.29.16	ABC	1	ESXi 5.5 < Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Productivo	No	0	8	24	0	24	24	No se gestiona	Medio	216
192.168.29.30	ABC	1	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Productivo	No	0	8	24	0	24	24	No se gestiona	Medio	217
192.168.29.57	XYZ	2	MS12-060: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2687502)	Low	3	Productivo	No	0	8	24	0	24	24	No se gestiona	Medio	218
192.168.29.88	DEF	9	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Productivo	No	0	7	21	0	21	21	No se gestiona	Bajo	219
192.168.29.55	XYZ	2	ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Productivo	No	0	7	21	0	21	21	No se gestiona	Bajo	220
192.168.29.72	ABC	3	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	221
192.168.29.72	ABC	3	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	222
192.168.29.78	ABC	9	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Critical	9	Productivo	No	0	2	18	0	18	18	4	Bajo	223
192.168.29.81	ABC	9	OpenSSL < 0.9.6l Denial of Service	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	224
192.168.29.53	DEF	1	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	225
192.168.29.53	DEF	1	Microsoft SQL Server Unsupported Version Detection	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	226
192.168.29.53	DEF	1	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	227
192.168.29.53	DEF	1	Unsupported Unix Operating System	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	228

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.60	DEF	2	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	229
192.168.29.60	DEF	2	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	230
192.168.29.60	DEF	2	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	231
192.168.29.60	DEF	2	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU)	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	232
192.168.29.60	DEF	2	Unsupported Unix Operating System	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	233
192.168.29.63	DEF	2	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	234
192.168.29.64	DEF	2	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	235
192.168.29.64	DEF	2	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	236
192.168.29.64	DEF	2	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	237
192.168.29.70	XYZ	3	MS09-050: Microsoft Windows SMB2 Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	238
192.168.29.70	XYZ	3	MS15-031: Security Update for Schannel to Address Spoofing (3061320)	Critical	9	Desarrollo	No	0	2	18	0	18	18	7	Bajo	239
192.168.29.50	DEF	1	OpenSSL < 0.9.8u Multiple Vulnerabilities	High	7	Desarrollo	No	0	2	14	0	14	14	8	Bajo	240
192.168.29.50	DEF	1	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	High	7	Desarrollo	No	0	2	14	0	14	14	8	Bajo	241
192.168.29.58	DEF	1	Apache < 1.3.31 / 2.0.48 Socket Connection Blocking Race Condition DoS	High	7	Pruebas	No	0	2	14	0	14	14	8	Bajo	242
192.168.29.60	DEF	2	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	High	7	Desarrollo	No	0	2	14	0	14	14	8	Bajo	243
192.168.29.64	DEF	2	Oracle 9iAS ISQLplus XSS	High	7	Pruebas	No	0	2	14	0	14	14	8	Bajo	244
192.168.29.70	XYZ	3	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation	High	7	Desarrollo	No	0	2	14	0	14	14	8	Bajo	245
192.168.29.125	ABC	10	MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	246
192.168.29.125	ABC	10	OpenSSL < 0.9.8k Denial of Service	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	247
192.168.29.58	DEF	1	OpenSSL < 0.9.8h Multiple Vulnerabilities	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	227
192.168.29.58	DEF	1	Unsupported Unix Operating System	Critical	9	Pruebas	No	0	2	18	0	18	18	7	Bajo	228

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.18	ABC	10	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	248
192.168.29.18	ABC	10	MS09-012: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	249
192.168.29.18	ABC	10	MS12-011: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	250
192.168.29.2	ABC	10	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) [uncredentialed check]	Medium	5	Productivo	No	0	2	10	0	10	10	6	Bajo	251
192.168.29.2	ABC	10	Web Server Expect Header XSS	Medium	5	Productivo	No	0	2	10	0	10	10	6	Bajo	252
192.168.29.25	ABC	10	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822538)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	253
192.168.29.34	ABC	1	OpenSSL c09.2y Multiple Vulnerabilities	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	254
192.168.29.38	ABC	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	255
192.168.29.40	ABC	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	256
192.168.29.71	ABC	3	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	257
192.168.29.71	ABC	3	Oracle Java JDK / JRE 6 c Update 30 Multiple Vulnerabilities	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	258
192.168.29.72	ABC	3	ESXi 5.5 c Build 1474526 File Descriptors Privilege Escalation [remote check]	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	259
192.168.29.46	DEF	9	Web Server Expect Header XSS	Medium	5	Productivo	No	0	2	10	0	10	10	6	Bajo	260
192.168.29.50	DEF	1	MS11-030: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) [remote check]	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	261
192.168.29.50	DEF	1	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822538)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	262
192.168.29.51	DEF	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) [uncredentialed check]	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	263
192.168.29.60	DEF	2	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	264
192.168.29.60	DEF	2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	265
192.168.29.60	DEF	2	OpenSSL c09.6f Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	266

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.60	DEF	2	Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	267
192.168.29.63	DEF	2	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	268
192.168.29.63	DEF	2	OpenSSL c09.2 Weak Default Configuration	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	269
192.168.29.63	DEF	2	Oracle Java JDK / JRE 6 c Update 30 Multiple Vulnerabilities	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	270
192.168.29.93	DEF	9	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	271
192.168.29.93	DEF	9	OpenSSL c09.2i Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	272
192.168.29.94	DEF	9	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	273
192.168.29.94	DEF	9	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	274
192.168.29.10	XYZ	1	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	275
192.168.29.104	XYZ	1	MS12-036: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	276
192.168.29.104	XYZ	1	OpenSSL c09.6f Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	277
192.168.29.104	XYZ	1	OpenSSL c09.2 Weak Default Configuration	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	278
192.168.29.104	XYZ	1	Web Server Expect Header XSS	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	279
192.168.29.117	XYZ	1	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	280
192.168.29.117	XYZ	1	Symantec AntiVirus Detection (Corporate Edition)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	281
192.168.29.12	XYZ	1	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	282
192.168.29.12	XYZ	1	OpenSSL c09.6k Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	283
192.168.29.13	XYZ	1	ESXi 5.5 c Build 1474526 File Descriptors Privilege Escalation (remote check)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	284
192.168.29.13	XYZ	1	Symantec AntiVirus Detection (Corporate Edition)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	285
192.168.29.60	DEF	2	Code Execution (958687)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	264
192.168.29.60	DEF	2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	265
192.168.29.60	DEF	2	OpenSSL c09.6f Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	266

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.26	XYZ	10	ESXi 5.5 c Build 1474526 File Descriptors Privilege Escalation [remote check]	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	286
192.168.29.26	XYZ	10	MS12-011: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	287
192.168.29.26	XYZ	10	Oracle 9iAS Nonexistent.jsp File Request Error Message Path Disclosure	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	288
192.168.29.41	XYZ	10	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) [uncredentialed check]	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	289
192.168.29.41	XYZ	10	OpenSSL c09.8 i Denial of Service	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	290
192.168.29.59	XYZ	10	OpenSSL c09.8 Weak Default Configuration	Medium	5	Productivo	No	0	2	10	0	10	10	6	Bajo	291
192.168.29.68	XYZ	10	OpenSSL c09.8 i Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	292
192.168.29.73	XYZ	9	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	293
192.168.29.51	DEF	1	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	9	Desarrollo	No	0	1	9	0	9	9	7	Bajo	294
192.168.29.51	DEF	1	Oracle Database Unsupported	Critical	9	Desarrollo	No	0	1	9	0	9	9	7	Bajo	295
192.168.29.51	DEF	1	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)	Critical	9	Desarrollo	No	0	1	9	0	9	9	7	Bajo	296
192.168.29.7	XYZ	3	ESXi 5.5 c Build 1623387 Multiple Vulnerabilities [remote check]	Critical	9	Pruebas	No	0	1	9	0	9	9	7	Bajo	297
192.168.29.7	XYZ	3	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	Critical	9	Pruebas	No	0	1	9	0	9	9	7	Bajo	298
192.168.29.7	XYZ	3	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Critical	9	Pruebas	No	0	1	9	0	9	9	7	Bajo	299
192.168.29.7	XYZ	3	Oracle Database Unsupported	Critical	9	Pruebas	No	0	1	9	0	9	9	7	Bajo	300
192.168.29.7	XYZ	3	Unsupported Unix Operating System	Critical	9	Pruebas	No	0	1	9	0	9	9	7	Bajo	301
192.168.29.51	DEF	1	OpenSSL c09.8 u Multiple Vulnerabilities	High	7	Desarrollo	No	0	1	7	0	7	7	8	Bajo	302
192.168.29.7	XYZ	3	OpenSSL 0.9.8 c 0.9.8x DTLS CBC Denial of Service	High	7	Pruebas	No	0	1	7	0	7	7	8	Bajo	303
192.168.29.2	ABC	10	ESXi 5.5 c Build 1980613 glibc Library Multiple Vulnerabilities [remote check]	Low	3	Productivo	No	0	2	6	0	6	6	No se gestiona	Bajo	304
192.168.29.18	XYZ	1	ESXi 5.5 c Build 1474526 File Descriptors Privilege Escalation [remote check]	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	284
192.168.29.18	XYZ	1	Symantec AntiVirus Detection [Corporate Edition]	Medium	5	Pruebas	No	0	2	10	0	10	10	9	Bajo	285
192.168.29.60	DEF	2	Code Execution [958687]	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	264
192.168.29.60	DEF	2	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	265
192.168.29.60	DEF	2	OpenSSL c09.6 f Denial of Service	Medium	5	Desarrollo	No	0	2	10	0	10	10	9	Bajo	266

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.2	ABC	10	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2689502)	Low	3	Productivo	No	0	2	6	0	6	6	No se gestiona	Bajo	305
192.168.29.25	ABC	10	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974445)	Low	3	Pruebas	No	0	2	6	0	6	6	No se gestiona	Bajo	306
192.168.29.40	ABC	1	OpenSSL 0.9.6m/0.9.7d Multiple Remote DoS	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	307
192.168.29.71	ABC	3	ESXi 5.5 c Build 1880813 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	308
192.168.29.71	ABC	3	OpenSSL SSL OP NETSCAPE REUSE CIPHER CHANGE BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	309
192.168.29.72	ABC	3	ESXi 5.5 c Build 1880813 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	310
192.168.29.81	ABC	9	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974445)	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	311
192.168.29.94	DEF	9	OpenSSL 0.9.6m/0.9.7d Multiple Remote DoS	Low	3	Pruebas	No	0	2	6	0	6	6	No se gestiona	Bajo	312
192.168.29.12	XYZ	1	ESXi 5.5 c Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	313
192.168.29.12	XYZ	1	MS13-053: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	314
192.168.29.15	XYZ	1	MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2689502)	Low	3	Pruebas	No	0	2	6	0	6	6	No se gestiona	Bajo	315
192.168.29.26	XYZ	10	OpenSSL 0.9.6m/0.9.7d Multiple Remote DoS	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	316
192.168.29.26	XYZ	10	OpenSSL SSL OP NETSCAPE REUSE CIPHER CHANGE BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	317
192.168.29.41	XYZ	10	ESXi 5.5 c Build 1880813 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Pruebas	No	0	2	6	0	6	6	No se gestiona	Bajo	318
192.168.29.59	XYZ	10	MS13-053: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Productivo	No	0	2	6	0	6	6	No se gestiona	Bajo	319
192.168.29.59	XYZ	10	OpenSSL 0.9.6m/0.9.7d Multiple Remote DoS	Low	3	Productivo	No	0	2	6	0	6	6	No se gestiona	Bajo	320
192.168.29.59	XYZ	10	OpenSSL SSL OP NETSCAPE REUSE CIPHER CHANGE BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Productivo	No	0	2	6	0	6	6	No se gestiona	Bajo	321
192.168.29.68	XYZ	10	OpenSSL SSL OP NETSCAPE REUSE CIPHER CHANGE BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	322
192.168.29.70	XYZ	3	OpenSSL SSL OP NETSCAPE REUSE CIPHER CHANGE BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	323

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V.x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V.x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.73	XYZ	9	OpenSSL c09 &m/ 0.9.7d Multiple Remote DoS	Low	3	Pruebas	No	0	2	6	0	6	6	No se gestiona	Bajo	324
192.168.29.89	ABC	1	MS08-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Productivo	No	0	1	5	0	5	5	6	Bajo	325
192.168.29.89	ABC	1	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Productivo	No	0	1	5	0	5	5	6	Bajo	326
192.168.29.89	ABC	1	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822338)	Medium	5	Productivo	No	0	1	5	0	5	5	6	Bajo	327
192.168.29.89	ABC	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042558)	Medium	5	Productivo	No	0	1	5	0	5	5	6	Bajo	328
192.168.29.27	ABC	1	MS12-011: Vulnerabilities in Microsoft Share Point Could Allow Elevation of Privilege (2663841)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	329
192.168.29.27	ABC	1	MS13-004: Vulnerabilities in Share Point Could Allow Elevation of Privilege (2780176)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	330
192.168.29.27	ABC	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042558)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	331
192.168.29.27	ABC	1	OpenSSL c09 &k Denial of Service	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	332
192.168.29.31	ABC	1	MS08-002: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	333
192.168.29.31	ABC	1	OpenSSL c09 &k Denial of Service	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	334
192.168.29.31	ABC	1	Web Server &pect Header XSS	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	335
192.168.29.35	ABC	1	MS14-074: Vulnerabilities in Microsoft Share Point Could Allow Elevation of Privilege (2451858)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	336
192.168.29.35	ABC	1	MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822338)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	337
192.168.29.35	ABC	1	OpenSSL c09 &k Denial of Service	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	338
192.168.29.35	ABC	1	Web Server &pect Header XSS	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	339
192.168.29.37	ABC	1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042558)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	340
192.168.29.39	ABC	1	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	341
192.168.29.48	ABC	1	MS08-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	342
192.168.29.68	XYZ	10	SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	322
192.168.29.70	XYZ	3	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	323

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x Valoración Tipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipInf Vs Normat) + V. x LAN) +Si es core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.79	ABC	9	OpenSSL c09 &f Denial of Service	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	343
192.168.29.80	ABC	9	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution |958687|	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	344
192.168.29.80	ABC	9	OpenSSL c09 &k Denial of Service	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	345
192.168.29.51	DEF	1	MS11-030: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) |remote check|	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	346
192.168.29.51	DEF	1	MS13-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (2042058)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	347
192.168.29.51	DEF	1	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	348
192.168.29.51	DEF	1	Web Server &pect Header XSS	Medium	5	Desarrollo	No	0	1	5	0	5	5	9	Bajo	349
192.168.29.53	DEF	9	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	350
192.168.29.95	DEF	9	OpenSSL c09 &k Denial of Service	Medium	5	Productivo	No	0	1	5	0	5	5	6	Bajo	351
192.168.29.96	DEF	9	MS12-011: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	352
192.168.29.96	DEF	9	MS12-056: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	353
192.168.29.96	DEF	9	MS13-085: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822338)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	354
192.168.29.97	DEF	9	MS12-011: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	355
192.168.29.97	DEF	9	OpenSSL c09 &l Multiple Vulnerabilities	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	356
192.168.29.97	DEF	9	Oracle Java JDK / JRE 6 c Update 30 Multiple Vulnerabilities	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	357
192.168.29.97	DEF	9	Symantec AntiVirus Detection (Corporate Edition)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	358
192.168.29.33	XYZ	10	MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	359
192.168.29.33	XYZ	10	Oracle Java JDK / JRE 6 c Update 30 Multiple Vulnerabilities	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	360
192.168.29.7	XYZ	3	MS13-085: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2822338)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	361
192.168.29.48	ABC	1	Code Execution |958687|	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	342
192.168.29.68	XYZ	10	SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	322
192.168.29.70	XYZ	3	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	2	6	0	6	6	No se gestiona	Bajo	323

IP	SW	VLAN	Vulnerabilidad	Criticidad	Valor Criticidad	Ambiente	Core	Valor por ser core	Valoración Tipo Inf Vs Normat	Resultado (ValorCriticidad x ValoraciónTipo Inf Vs Normat)	Valoración por Red	Suma (V.Crit.x V. TipoInf Vs Normat) + V. x LAN	Suma ((V.Crit.x V. TipoInf Vs Normat) + V. x LAN) +Sies core	OrdenGestión Vulnerabilidades Escenario Actual	Criticidad Escenario 2	OrdenGestión Vulnerabilidades Escenario Propuesto
192.168.29.7	XYZ	3	OpenSSL c09.8 i Denial of Service	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	362
192.168.29.7	XYZ	3	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Medium	5	Pruebas	No	0	1	5	0	5	5	9	Bajo	363
192.168.29.89	ABC	1	ESXi 5.5 c Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Productivo	No	0	1	3	0	3	3	Nos egestiona	Bajo	364
192.168.29.89	ABC	1	MS12-090: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2689502)	Low	3	Productivo	No	0	1	3	0	3	3	Nos egestiona	Bajo	365
192.168.29.89	ABC	1	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Productivo	No	0	1	3	0	3	3	Nos egestiona	Bajo	366
192.168.29.27	ABC	1	MS12-090: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2689502)	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	367
192.168.29.35	ABC	1	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	368
192.168.29.37	ABC	1	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	369
192.168.29.39	ABC	1	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974445)	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	370
192.168.29.39	ABC	1	OpenSSL c09.6 m/ 0.9.7d Multiple Remote DoS	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	371
192.168.29.43	ABC	1	ESXi 5.5 c Build 1580613 glibc Library Multiple Vulnerabilities (remote check)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	372
192.168.29.43	ABC	1	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974445)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	373
192.168.29.51	DEF	1	ESXi 5.5 c Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	374
192.168.29.51	DEF	1	OpenSSL c09.6 m/ 0.9.7d Multiple Remote DoS	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	375
192.168.29.51	DEF	1	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Desarrollo	No	0	1	3	0	3	3	Nos egestiona	Bajo	376
192.168.29.53	DEF	9	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	377
192.168.29.96	DEF	9	ESXi 5.5 c Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	378
192.168.29.97	DEF	9	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	379
192.168.29.33	XYZ	10	ESXi 5.5 c Build 1331737 OpenSSL Library Multiple Vulnerabilities (remote check)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	380
192.168.29.7	XYZ	3	MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974445)	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	381
192.168.29.7	XYZ	3	OpenSSL SSL OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Low	3	Pruebas	No	0	1	3	0	3	3	Nos egestiona	Bajo	382